# Autour de la conjecture de parité

Thomas de La Rochefoucauld

Université Paris VI - Pierre et Marie Curie

**École Doctorale Paris Centre**

# Thèse de doctorat

Discipline : Mathématiques

présentée par

**Thomas de La Rochefoucauld**

---

## Autour de la conjecture de parité

---

dirigée par Jan Nekovář

Soutenue le 22 octobre 2012 devant le jury composé de :

| | | |
|---|---|---|
| Daniel Bertrand | Université Paris 6 | Examinateur |
| David Burns | King's College, Londres | Rapporteur |
| Guy Henniart | Université Paris 11 | Examinateur |
| Marc Hindry | Université Paris 7 | Examinateur |
| Jan Nekovář | Université Paris 6 | Directeur |

Institut de Mathématiques de Jussieu
175, rue du chevaleret
75 013 Paris

École doctorale Paris centre Case 188
4 place Jussieu
75 252 Paris cedex 05

# Remerciements

*Paris, le 1 Octobre 2012*

Je tiens, avant toute chose, à remercier Jan Nekovář pour avoir accepté de me guider pendant ces 4 années. Il était toujours disponible lorsque j'avais besoin de lui. Ses réponses et ses explications sont toujours d'une grande acuité (même si parfois il me faut un peu de temps pour m'en rendre compte). Je tiens aussi à le remercier vivement pour son investissement dans la lecture attentive et les remarques concernant mes notes et articles personnels et bien sûr la présente thèse.

J'ai eu la chance de pouvoir enseigner pendant toute ma thèse. C'est une activité qui me tient à coeur et je tiens ici à remercier toutes les personnes avec lesquelles j'ai travaillé dans ce cadre ainsi que les étudiants qui j'espère auront pris autant de plaisir que moi.

Je tiens à remercier aussi les professeurs qui m'ont guidé jusqu'ici au cours de mes études et tout spécialement Marc Hindry qui m'a initié notamment aux courbes elliptiques et qui, avec une grande gentillesse et de grandes qualités mathématiques, avait encadré mon mémoire de Master.

Au cours de ma thèse, j'ai eu notamment la chance de passer un mois au Etats-Unis dans le cadre d'une école d'été sur "l'arithmétique des fonctions $L$" organisée par l'IAS. A cette occasion, j'ai eu le plaisir de rencontrer (malheureusement trop brièvement) le professeur David Rohrlich et de suivre un de ses cours. J'ai beaucoup d'admiration pour son travail et la qualité d'expositions de ses articles.

Je remercie vivement les professeurs David Rohrlich et David Burns d'avoir accepté de rapporter cette thèse. Le jour de la soutenance est un jour très particulier pour un doctorant et je remercie Daniel Bertrand, David Burns, Marc Hindry et Guy Henniart d'avoir accepté d'y participer en faisant partie de mon jury.

Cette thèse doit beaucoup (le lecteur attentif s'en rendra très vite compte) aux travaux de Tim et Vladimir Dokchitser. Si je remercie Vladimir d'avoir répondu aux questions que je lui avais posées sur un de leurs articles, mes remerciements vont tout spécialement à Tim que j'ai rencontré au CRM de Barcelone et qui a montré beaucoup d'intérêt et m'a poussé à publier ce qui était mon premier résultat et qui constitue le chapitre 4 de cette thèse.

Je tiens à remercier l'ensemble de l'école doctorale et tout particulièrement Corentin Lacombe qui m'a parfaitement accompagné dans toutes les démarches à effectuer avant la soutenance.

Il va sans dire que les collègues et amis thésards sont très importants durant toute la durée d'une thèse. Je tiens à remercier les gens que j'ai cotoyé à Chevaleret puis à Jussieu. Notamment Louis-Hadrien (que j'ai retrouvé en thèse alors même que nous avions été dans le même lycée), Johan (qui m'a initié à l'escalade), Paloma (qui était du voyage au Etats-Unis), Pierre-Guy, Juliette, Laura, Delphine, Giovanni, Nicolas, Pierre, Benjamin et plus récemment Florent, Clément, Anne-Sandrine, Henri, Charles, Clémence, Lara, Nicolas,

Jean, les François et tant d'autres.

J'ai bien sur une pensée particulière pour mon groupe d'amis de longue date qu'il m'est arrivé de "saouler" avec "mes maths" et spécialement pour Arnaud qui m'a accompagné longtemps en mathématiques. Une pensée aussi pour Léo qui était avec moi en licence et qui a repris l'an dernier les études en L3 après 6 années d'absence dans l'optique de faire une thèse par la suite. La route est encore longue mais je ne doute pas qu'il prendra la relève, bon courage !

Si ce n'est pas mes parents qui m'ont initié aux mathématiques, je leur dois énormément et je profite de ces lignes pour les remercier pour tout ce qu'ils ont fait et font encore pour moi. Je pense bien sûr à mon petit frère Arthuro... avec qui je partage beaucoup et qui croit toujours en moi. Enfin, je remercie Charlotte qui partage ma vie depuis près de 5 ans et m'a supporté (et supporté...) pendant toute cette thèse.

# Table des matières

# Introduction

C'est en 1922 que Louis Mordell, répondant à une question posée en 1908 par Henri Poincaré, démontre que le groupe des points rationnels d'une courbe elliptique définie sur $\mathbb{Q}$ est finiment engendré. En 1928, André Weil dans sa thèse de doctorat étend le résultat aux courbes elliptiques définies sur un corps de nombres quelconque (il étend même le résultat aux variétés abéliennes qui sont des jacobiennes de courbes). Pour une courbe elliptique définie sur un corps de nombres $K$, ceci revient à dire que :

$$E(K) \simeq \mathbb{Z}^{r_{E/K}} \times E(K)_{tors}$$

où $E(K)_{tors}$ désigne les points de torsion (c'est un groupe abélien fini) et $r_{E/K}$ s'appelle le rang de la courbe $E/K$. On a, aujourd'hui, une description relativement précise de $E(K)_{tors}$, notamment grâce aux travaux de B. Mazur (dans [31] et [32]) et L. Merel (dans [33]). Le rang $r_{E/K}$ demeure très largement mystérieux.

Dans le début des années 1960, à la suite d'une expérience sur ordinateur (parmi les premières en mathématiques), Brian Birch et Peter Swinnerton-Dyer ont énoncé une conjecture reliant le rang d'une courbe elliptique à l'ordre d'annulation de la fonction $L$ associée à la courbe : la, désormais célèbre, conjecture de Birch-Swinnerton-Dyer. Les questions traitées dans cette thèse ont pour point de départ cette conjecture.

## 0.1 La conjecture de Birch-Swinnerton-Dyer

Soit $K$ un corps de nombres et $E$ une courbe elliptique sur $K$. Notons $K_v$ la complétion de $K$ à la place $v$.

Le module de Tate $l$-adique $T_l(E)$ de $E$ (plus précisément $V_l(E) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(E)$) donne lieu pour toute place $v$ à une représentation du groupe de Galois absolu de $K_v$ $\sigma'_{E/K_v,l} : Gal(\overline{K}_v/K_v) \longrightarrow GL(V_l(E)^*)$. Si on fixe un plongement $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$, on obtient une représentation complexe $\sigma'_{E/K_v,l,\iota}$ du groupe de Weil-Deligne $\mathcal{WD}_{K_v}$ de $K_v$ (la classe d'isomorphie de $\sigma'_{E/K_v} := \sigma'_{E/K_v,l,\iota}$ est indépendante du choix de $l$ et de $\iota$).

Notons $L(E/K, s)$ la fonction $L$ globale, produit des fonctions $L$ locales :

$$L(E/K, s) = \prod_{v \text{ finies}} L(E/K_v, s) \left( := \prod_{v \text{ finies}} L(\sigma'_{E/K_v}, s) \right)$$

définie pour $\mathrm{Re}(s) > \dfrac{3}{2}$ (voir la section 2.2.2 du chapitre 2 pour la définition de $L(E/K_v, s)$) et par

$$\Lambda(E/K, s) = A(E/K)^{s/2} L(E/K, s)(2(2\pi)^{-s}\Gamma(s))^{[K:\mathbb{Q}]},$$

la fonction $L$ complète où $A(E/K)$ est une constante qui s'exprime en fonction du discriminant et du conducteur de $E/K$ et où $(2(2\pi)^{-s}\Gamma(s))^{[K:\mathbb{Q}]}$ est le facteur qui correspond au produit $\prod_{v \text{ infinies}} L(\sigma'_{E/K_v}, s)$ (voir la section 2.5 du chapitre 2).

On peut désormais énoncer la conjecture suivante :

**Conjecture 0.1.1.** (Equation fonctionnelle de $\Lambda$ : FE) :
$\Lambda(E/K,s)$ admet un prolongement holomorphe à $\mathbb{C}$ et il existe un signe

$$W(E/K)=\prod_v W(E/K_v)\in\{\pm 1\}$$

tel que :

$$\Lambda(E/K,s)=W(E/K)\Lambda(E/K,2-s)$$

(voir la section 2.4 pour la définition de $W(E/K_v):=W(\sigma'_{E/K_v})$ aux places finies, la section 2.5 pour la définition aux places archimédiennes et [45] §21 p.157 pour l'équation fonctionnelle de $\Lambda$).

**Remarque 0.1.2.** Cette conjecture est connue dans quelques cas :
· Pour les courbes elliptiques sur $\mathbb{Q}$ grâce aux résultats de modularité dus à Wiles, Taylor, Breuil, Diamond et Conrad.
· Pour les courbes elliptiques sur un corps de nombres totalement réel, on sait que $\Lambda$ admet un prolongement méromorphe et satisfait l'équation fonctionnelle grâce à un résultat de modularité potentiel de Wintenberger (voir [64]) joint à un argument de Taylor.
Dans le cas général, cette conjecture n'est pas connue.

Si $\Lambda(E/K,s)$ admet un prolongement holomorphe à $\mathbb{C}$ alors on peut parler de l'ordre d'annulation de $\Lambda$ en $s=1$ et énoncer la conjecture de Birch et Swinnerton-Dyer :

**Conjecture 0.1.3.** (Birch et Swinnerton-Dyer : BSD) :

$$ord_{s=1}\Lambda(E/K,s)=rg(E/K).$$

**Remarque 0.1.4.** On a seulement quelques éléments concernant cette conjecture, notamment :
· B. Gross et D. Zagier ont montré en 1986 qu'une courbe elliptique modulaire dont l'ordre d'annulation en $s=1$ est 1 admet un point rationnel.
· Kolyvagin a montré en 1989 qu'une courbe elliptique modulaire, dont l'ordre d'annulation en $s=1$ est 0, est de rang 0.
· Grâce aux résultats de modularité des courbes elliptiques sur $\mathbb{Q}$, les deux précédents sont valables pour des courbes elliptiques sur $\mathbb{Q}$.

Les deux premiers chapitres de cette thèse sont des chapitres de rappels qui permettent notamment au chapitre 3 d'énoncer une généralisation de cette conjecture (la conjecture de Bloch-Kato) et les conjectures de parité (dans un cadre plus vaste que celui des seules courbes elliptiques) dont nous allons dire quelques mots tout de suite.

## 0.2 Les conjectures de parité et de $p$-parité

La conjecture de Birch et Swinnerton-Dyer implique la conjecture plus faible suivante :

**Conjecture 0.2.1.** (BSD $(\mathrm{mod}\,2)$)

$$rg(E/K)\equiv ord_{s=1}\Lambda(E/K,s)\,(\mathrm{mod}\,2)\,.$$

Combinée avec l'équation fonctionnelle conjecturale on obtient :

**Conjecture 0.2.2.** (Conjecture de parité)

$$(-1)^{rg(E/K)} = W(E/K).$$

Tim et Vladimir Dokchitser ont montré que cette conjecture est vraie si on suppose que la partie de $6^\infty$-torsion du groupe de Tate-Shafarevich de $E$ sur $K(E[2])$ est finie (voir [21] Th 7.1 p.20).

**Définition 0.2.3.** Groupe de Selmer :
Soit

$$X_p(E/K) := Hom_{\mathbb{Z}_p}(S(E/K, p^\infty), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

où $S(E/K, p^\infty) := \varinjlim_n S(E/K, p^n)$ est le $p^\infty$-groupe de Selmer, qui apparaît dans la suite exacte suivante :

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow S(E/K, p^\infty) \longrightarrow Ш_{E/K}[p^\infty] \longrightarrow 0.$$

Si on pose $\mathrm{rg}_p(E/K) := \dim_{\mathbb{Q}_p} X_p(E/K) = rg(E/K) + \mathrm{cork}_{\mathbb{Z}_p} Ш_{E/K}[p^\infty]$, on a la version plus accessible suivante de la Conjecture :

**Conjecture 0.2.4.** (Conjecture de $p$-parité)

$$(-1)^{rg_p(E/K)} = W(E/K).$$

**Remarque 0.2.5.** Cette version est plus accessible car elle ne nécessite pas la connaissance du groupe de Tate-Shafarevitch dont on sait peu de choses. Les résultats connus sur la conjecture de parité sont conditionnels à la finitude de Ш. C'est en général la conjecture de $p$-parité qui est établie (pour certains $p$), la conjecture de parité en découlant directement si on suppose la finitude de Ш.

Si $L/K$ est une extension galoisienne finie et $\tau$ est une $\overline{\mathbb{Q}}_p$-représentation auto-duale de $Gal(L/K)$ alors on peut énoncer une version équivariante de la conjecture :

**Conjecture 0.2.6.** (Conjecture de $p$-parité avec twist (auto-duale))

$$(-1)^{\langle \tau, X_p(E/L)\rangle} = W(E/K, \tau),$$

où $W(E/K, \tau) = \prod_v W(\sigma'_{E/K_v} \otimes \mathrm{Res}_{D_v} \tau)$, $D_v \subset Gal(L/K)$ est le groupe de décomposition en $v$ et $\langle \tau, * \rangle$ est le produit scalaire classique des caractères de $\tau$ et du complexifié de $*$.

Dans le chapitre 4 de cette thèse on obtient des résultats concernant ces deux dernières conjectures. On démontre le résultat clef suivant :

**Théorème 0.2.7.** Soit $K$ un corps de nombres, $E/K$ une courbe elliptique et $L/K$ une extension galoisienne finie tel que $Gal(L/K) \simeq D_{2p^n}$, avec $p \geq 5$ un nombre premier. La conjecture de $p$-parité pour $E/K$ tensorisé par $1 \oplus \eta \oplus \tau$ est vérifiée, c'est à dire :

$$W(E/K, 1 \oplus \eta \oplus \tau) = (-1)^{\langle 1 \oplus \eta \oplus \tau, X_p(E/L)\rangle}$$

où 1 est la représentation triviale, $\eta$ le caractère quadratique et $\tau$ une représentation irréductible de degré 2 de $Gal(L/K)$.

**Remarque 0.2.8.** Un résultat analogue a été démontré par Tim et Vladimir Dokchitser avec des hypothèses supplémentaires (voir notamment la remarque 4.1.11 au chapître 4).

Ce théorème permet de démontrer (grâce aux travaux des frères Dokchitser) notamment les deux théorèmes suivants concernant les conjectures de $p$-parité et de $p$-parité avec twist :

**Théorème 0.2.9.** Soit $K$ un corps de nombres, $p \geq 3$, et $E/K$ une courbe elliptique. Supposons que $F$ est une $p$-extension d'une extension galoisienne $M/K$, galoisienne sur $K$. Si la conjecture de $p$-parité

$$(-1)^{\mathrm{rk}_p\, E/L} = W(E/L)$$

est vérifiée pour tout sous-corps $K \subset L \subset M$, alors elle est vérifiée pour tout sous-corps $K \subset L \subset F$.

**Corollaire 0.2.10.** Soit $E/\mathbb{Q}$ une courbe elliptique et $p \geq 3$. Supposons que $F$ est une $p$-extension d'une extension quadratique $M/\mathbb{Q}$, galoisienne sur $\mathbb{Q}$ alors

$$(-1)^{\mathrm{rk}_p\, E/L} = W(E/L)$$

pour tout sous-corps $L$ de $F$.

**Théorème 0.2.11.** Soit $K$ un corps de nombres, $p \geq 3$, $E/K$ une courbe elliptique et $F/K$ une extension galoisienne. Supposons que le $p$-sous-groupe de $P$ de $G = Gal(F/K)$ est distingué et que $G/P$ est abélien. Si la conjecture de $p$-parité est vérifiée pour $E$ sur $K$ et ses extensions quadratiques dans $F$, alors elle est vérifiée pour tout twist de $E$ par une représentation orthogonale de $G$.

## 0.3 Une généralisation de la formule de Rohrlich pour les signes locaux

Les résulats obtenus ci-dessus reposent de façon essentielle sur une formule de David. E. Rohrlich pour $W(E/K_v, \tau)$ où $\tau$ est une représentation auto-duale. Le résultat clef que Rohrlich a démontré dans [46] est le théorème suivant :

**Théorème 0.3.1.** Soit $E$ une courbe elliptique sur $K_v$ et $\tau$ une représentation auto-duale de $G_K$ alors :

1. Si $E$ a réduction potentiellement multiplicative alors :

$$W(E/K_v, \tau) = (\det \tau)(-1)\chi(-1)^{\dim \tau}(-1)^{\langle \chi, \tau \rangle}$$

   où $\chi$ est le caractère de $K_v^\times$ associé à l'extension $K_v(\sqrt{c_6})$ de $K_v$ (i.e le corps où $E$ acquiert réduction multiplicative déployée).

2. Si $E$ a potentiellement bonne réduction alors $\sigma'_{E/K_v} = \sigma_{E/K_v}$ est une représentation de $\mathcal{W}_{K_v}$ et si $l_v \geq 5$ on a :

$$W(E/K_v, \tau)) = \begin{cases} (\det \tau)(-1)(-W(E/K_v))^{\dim \tau}(-1)^{\langle 1+\eta+\hat{\sigma}, \tau \rangle} & \text{si } \sigma_{E/K} \text{ est irréd,} \\ (\det \tau)(-1)(W(E/K_v))^{\dim \tau} & \text{sinon.} \end{cases}$$

La quantité $W(E/K_v, \tau) := W(\sigma'_{E/K} \otimes \tau)$ étant définie à l'aide de la représentation essentiellement symplectique du groupe de Weil-Deligne $\sigma'_{E/K_v} : \mathcal{WD}_{K_v} \longrightarrow GL(V_l(E)^*)$,

il est légitime de chercher une formule équivalente dans le cas d'une représentation essentiellement symplectique plus générale de $\mathcal{WD}_{K_v}$. Nous donnons au chapitre 5 une formule qui généralise la formule du point 2. du théorème précédent. En effet, on donne une formule dans le cas où la représentation de $\mathcal{WD}_{K_v}$ se factorise à travers une représentation essentiellement symplectique, modérement ramifiée du groupe de Weil $\mathcal{W}_{K_v}$. Précisément, on obtient :

**Théorème 0.3.2.** Soit $\sigma$ est une représentation essentiellement symplectique de poids $w$ et modérement ramifiée de $\mathcal{W}_{K_v}$, $l_v \neq 2$ et $\tilde{\sigma} = \sigma \otimes \omega^{w/2}$ alors pour toute représentation (complexe) auto-duale $\tau$ de $G_{K_v}$ :

$$W(\sigma \otimes \tau) = \begin{cases} (\det \tau(-1))^{\frac{\dim \sigma}{2}} (-W(\sigma))^{\dim \tau} (-1)^{\langle 1 \oplus \eta_{nr} \oplus \rho, \tau \rangle} & \text{si } \tilde{\sigma} \text{ est sympl et irréd,} \\ (\det \tau(-1))^{\frac{\dim \sigma}{2}} W(\sigma)^{\dim \tau} & \text{si } \tilde{\sigma} = \theta \oplus \theta^* \end{cases}$$

**Remarque 0.3.3.** Si $E/K_v$ est une courbe ayant potentiellement bonne réduction alors si $l_v \geq 5$, la représentation $\sigma'_{E/K_v}$ est une représentation modérément ramifiée de dimension 2 de $\mathcal{W}_{K_v}$ et en appliquant le théorème ci-dessus, on retrouve le résultat de Rohrlich.

## 0.4 Nombres de Tamagawa et constantes de régulation

Les résultats sur les conjectures de $p$-parité et de $p$-parité avec twist du chapitre 4 repose sur le travail des frères Dokchitser dans [18] et notamment le résultat clef de cet article (Théorème 3.2) qui lie (à l'aide de la formule de Rohrlich) les nombres de Tamagawa et ce qu'ils appellent les constantes de régulation. Ce résultat, un peu technique, est rappellé à la fin du chapitre 3. Ce théorème de nature locale repose notamment sur la connaissance de la forme explicite du groupe de Galois du corps sur lequel la courbe admet une réduction semi-stable. Ces groupes, peu nombreux, ont pour cardinal une puissance de 2 fois une puissance de 3 (en particulier, il en est de même pour son sous-groupe d'inertie).Partant d'une courbe elliptique sur un corps de nombres, il s'avère que le fait que la famille des représentations $\sigma'_{E/K_v}$ pour les différentes place $v$ de $K$ soit prémotivique (ou fortement compatible, voir la définition 1.4.6) impose cette condition sur le cardinal du groupe d'inertie. Après avoir introduit au chapitre 1 ce que nous entendons par prémotif (ou famille fortement compatible), dans le chapitre 6 (avec l'aide de la formule obtenue au chapitre 5) nous généralisons le lien entre nombres de Tamagawa et constantes de régulation à un prémotif essentiellement symplectique quelconque dans le cas modéré où $p \neq l_v$.

# Chapitre 1

# Représentations galoisiennes et prémotifs

## 1.1 Corps locaux et groupes de Weil

On rappelle la définition de $\mathbb{Q}_l$.

**Définition 1.1.1.** Si $l$ est un nombre premier, $\mathbb{Q}_l$ est la complétion de $\mathbb{Q}$ relativement à la distance $l$-adique $d_l(x,y) = |x-y|_l$ où si $\frac{a}{b} \in \mathbb{Q}$, $|\frac{a}{b}|_l = l^{v_l(b)-v_l(a)}$.

**Remarque 1.1.2.**

1. On peut définir $\mathbb{Q}_l$ de façon équivalente comme le corps des fractions de $\mathbb{Z}_l = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/l^n\mathbb{Z}$ où $\varprojlim_{n\in\mathbb{N}}$ désigne la limite projective.
2. Le corps $\mathbb{Q}_l$ est localement compact.
3. L'anneau $\mathbb{Z}_l$ possède un unique idéal maximal $l\mathbb{Z}_l$.
4. Les idéaux $l^n\mathbb{Z}_l$ forment une base de voisinage de 0.
5. On a $\mathbb{Z}_l = \{\alpha \in \mathbb{Q}_l \,||\alpha|_l \leq 1\}$ et $l\mathbb{Z}_l = \{\alpha \in \mathbb{Q}_l \,||\alpha|_l < 1\}$.

**Définition 1.1.3.** On appellera corps local une extension finie d'un $\mathbb{Q}_l$.

**Remarque 1.1.4.** Il est courant de considérer plus de corps dans la notion de corps local :

1. Les corps locaux en caractéristique 0.
   (a) Archimédien : $\mathbb{R}$ et $\mathbb{C}$.
   (b) Non archimédien : les extensions finies des $\mathbb{Q}_l$ (les "nôtres").
2. Les corps locaux en caractéristique positive : les extensions finies des $\mathbb{F}_p((t))$.

**Définition 1.1.5.** Si $K$ est une extension finie de $\mathbb{Q}_l$ de degré $n$ ($[K:\mathbb{Q}_l] = n$) alors on note :

- Pour $\alpha \in K$, $v_K(\alpha) = \frac{1}{n} v_l(N_{K/\mathbb{Q}_l}(\alpha))$ et , $|\alpha|_K = l^{-v_K(\alpha)}$.
- l'anneau $\mathcal{O}_K := \{\alpha \in K \mid |\alpha|_K \leq 1\}$ est un sous-anneau ouvert et compact de $K$ appellé anneau des entiers de $K$.
- Le groupe $\mathcal{O}_K^\times := \{\alpha \in K \mid |\alpha|_K = 1\}$ est le groupe des unités de $\mathcal{O}_K$.

L'anneau $\mathcal{O}_K$ vérifie les propriétés suivantes :

1. L'anneau $\mathcal{O}_K$ possède un unique idéal maximal $\mathfrak{m}_K := \{\alpha \in K \mid |\alpha|_K < 1\}$. Cet idéal $\mathfrak{m}_K$ est principal et engendré par une uniformisante $\varpi_K$.

2. On a $\mathcal{O}_K = \varprojlim_{n\in\mathbb{N}} \mathcal{O}_K/\mathfrak{m}_K^n$.
3. Le quotient $k_K := \mathcal{O}_K/\mathfrak{m}_K$ est un corps fini, extension de $\mathbb{Z}_l/l\mathbb{Z}_l \simeq \mathbb{F}_l$. $\#k_K = q_K = l^{f_K}$ où $f_K$ est appelé le degré résiduel de $K/\mathbb{Q}_l$.
4. On a $l\mathcal{O}_K = \mathfrak{m}_K^{e_K}$ où $e_K$ est appelé le degré de ramification de $K/\mathbb{Q}_l$.
5. On a l'égalité $[K : \mathbb{Q}_l] = e_K f_K$.
6. Si $L/K$ est une extension finie de $K$. $k_L$ est une extension finie de $k_K$, on note $[k_L : k_K] = f_{L/K}$ et $\mathfrak{m}_K = \mathfrak{m}_L^{e_{L/K}}$. On appelle $f_{L/K}$ (resp $e_{L/K}$) le degré résiduel (resp de ramification) de $L/K$ et on a :

$$f_{L/K} = f_L/f_K,\ e_{L/K} = e_L/f_K \text{ et } [L : K] = e_{L/K} f_{L/K}$$

On dira que $L/K$ est non ramifié si $e_{L/K} = 1$.

**Définition-Proposition 1.1.6.** Soit $L/K$ est une extension galoisienne ($L$ et $K$ deux extensions de $\mathbb{Q}_l$). On a un morphisme surjectif de $Gal(L/K)$ dans $Gal(k_L/k_K)$ dont le noyau, noté $I_{L/K}$ est appellé le groupe d'inertie de $L$ sur $K$. On a alors la suite exacte suivante :

$$0 \longrightarrow I_{L/K} \longrightarrow Gal(L/K) \xrightarrow{\pi} Gal(k_L/k_K) \longrightarrow 0.$$

On remarquera que $L/K$ est non ramifié si et seulement si $\pi$ est un isomorphisme.

**Remarque 1.1.7.** Le groupe $Gal(k_L/k_K)$ est un groupe cyclique engendré par le morphisme de Frobenius : $fr : x \mapsto x^{|k_K|}$ où $|k_K|$ est le cardinal de $k_K$. De façon équivalente, il est engendré par $\varphi : x \mapsto x^{-|k_K|}$ l'inverse du Frobenius $fr$. On appelle $\varphi$ le *Frobenius géométrique*.

**Théorème 1.1.8.** Soit $K$ une extension finie de $\mathbb{Q}_l$ (non nécessairement galoisienne) et soit $k$ une extension finie de $k_K$ (de degré $f$). Alors il existe une extension non ramifiée $L$ de $K$ telle que $k_L \simeq k$. Une telle extension est unique à $K$-isomorphisme près et galoisienne sur $K$. On la notera $K_f$.

**Définition 1.1.9.** Fixons $\bar{K}$ une clôture algébrique de $K$. La famille des extensions non-ramifiées $K_f$ forme un système inductif de sous-corps de $\bar{K}$. Leur limite inductive (union) est un corps nommé l'extension maximale non-ramifée de $K$ et on la note $K_{nr}$. On a alors la suite exacte suivante :

$$0 \longrightarrow I_K \longrightarrow Gal(\bar{K}/K) \xrightarrow{\pi} Gal(K_{nr}/K) \longrightarrow 0$$

où $I_K$, le noyau de $\pi$, est le sous-groupe d'inertie de $Gal(\bar{K}/K)$.

**Théorème 1.1.10.** Toute extension finie de $K$ incluse dans $K_{nr}$ est non-ramifiée. On a la suite exacte suivante :

$$0 \longrightarrow I_K \longrightarrow Gal(\bar{K}/K) \xrightarrow{\pi} Gal(\bar{k}_K/k_K) \longrightarrow 0$$

où $Gal(\bar{k}_K/k_K) \simeq Gal(K_{nr}/K)$ et $I_K \simeq \varprojlim_{L/K} I_{L/K}$ (la limite étant prise sur les extensions galoisiennes finies).

**Remarque 1.1.11.** Comme $Gal(\bar{k}_K/k_K) \simeq \varprojlim_{k/k_K} Gal(k/k_K) \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} \simeq \prod_p \mathbb{Z}_p =: \hat{\mathbb{Z}}$ (où la première limite est prise sur les extensions galoisiennes finies et pour l'isomorphisme du milieu on a choisi le Frobenius géométrique $\varphi$ comme générateur de $Gal(k/k_K)$), on peut réecrire la suite exacte ci-dessus :

$$0 \longrightarrow I_K \longrightarrow Gal(\bar{K}/K) \xrightarrow{\pi} \hat{\mathbb{Z}} \longrightarrow 0. \tag{1}$$

**Définition 1.1.12.** Le groupe de Weil de $K$ est défini par : $\mathcal{W}_K := \mathcal{W}(\bar{K}/K) = \pi^{-1}(\mathbb{Z})$ (où $\mathbb{Z}$ s'identifie au sous-groupe de $Gal(\bar{k}_K/k_K) \simeq \hat{\mathbb{Z}}$ engendré par le Frobenius) et on a la suite exacte suivante

$$0 \longrightarrow I_K \xrightarrow{i} \mathcal{W}_K \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0. \tag{2}$$

On met sur $\mathbb{Z}$ la topologie discrète et sur $W_K$ la topologie qui rend $\pi$ continu et $I_K$ homéomorphe à $\pi^{-1}(\{0\})$.

**Remarque 1.1.13.**

1. On note parfois $\mathcal{W}_{k_K}$ le sous-groupe de $Gal(\bar{k}_K/k_K)$ engendré par le Frobenius.
2. On notera $\Phi$ un antécédent de $\varphi$ (l'inverse du Frobenius) par $\pi$ et on appellera $\Phi$ un Frobenius géométrique.
3. Le groupe $Gal(\bar{K}/K)$ est compact (comme groupe profini), $I_K$ est le noyau de $\pi$ (qui est continu) donc fermé dans $Gal(\bar{K}/K)$, donc $I_K$ est compact.
4. La topologie sur $\mathcal{W}_K$ est la plus grossière qui rend $i$ et $\pi$ continus.
5. Attention, la topologie qu'on vient de définir sur $\mathcal{W}_K$ ne coïncide pas avec la topologie induite par $G_K := Gal(\bar{K}/K)$.
6. Pour cette topologie, certains sous groupes ouverts (par exemple $I_K$) ne sont pas d'indice fini (contrairement au cas des groupes compacts comme $I_K$ et $Gal(\bar{K}/K)$).
7. L'identité admet une base de voisinage formée de sous-groupes ouverts de $I_K$.

## 1.2 Théorie du corps de classes local

### 1.2.1 Loi de réciprocité locale

On rappelle dans cette partie les résultats principaux de la théorie du corps de classes (local) puis on les énonce en fonction du groupe de Weil.

Soit $K$ une extension finie de $\mathbb{Q}_l$.

**Théorème 1.2.1.** Si $L/K$ est une extension galoisienne finie, alors on a un isomorphisme canonique $r_{L/K} : Gal(L/K)^{ab} \xrightarrow{\sim} K^\times/N_{L/K}(L^\times)$ où $N_{L/K} : L \longrightarrow K$ désigne la norme de $L$ sur $K$

**Démonstration.** Voir le théorème 1.3 p.320 de [41]. ■

L'isomorphime réciproque $\theta_{L/K} : K^\times/N_{L/K}(L^\times) \longrightarrow Gal(L/K)^{ab}$ est appelé l'application de réciprocité locale d'Artin (classique).

Pour $x \in K^\times$, on note $(x, L/K) = \theta_{L/K}(\bar{x}^{-1})$ (où $\bar{x}$ désigne la classe de $x$ dans le quotient $K^\times/N_{L/K}(L^\times)$). On a précomposé $\theta_{L/K}$ par $x \longrightarrow x^{-1}$ pour avoir une normalisation adaptée au Frobenius géométrique (voir la remarque 1.1.13).

Pour $L'/L/K$ extensions abéliennes, les morphismes $(,L/K) : K^\times \longrightarrow Gal(L/K)$ sont compatibles et en prenant la limite projective on obtient un morphisme $\theta_K : K^\times \longrightarrow Gal(\bar{K}/K)^{ab}$. La suite exacte (1) donne naissance à la suite exacte suivante :

$$0 \longrightarrow I_{K^{ab}/K} \longrightarrow Gal(K^{ab}/K) \xrightarrow{\pi^{ab}} \hat{\mathbb{Z}} \longrightarrow 0.$$

Pour $L/K$ une extension non ramifiée et $x \in K^\times$, on définit $v(x)$ par $|x|_K = q_K^{v(x)}$ et on note $\Phi : y \longrightarrow y^{-q_K} \in Gal(L/K)$ le Frobenius géométrique (on notera que c'est précisément l'image d'un élément $\Phi$ de $\mathcal{W}_K$ qu'on a défini dans la remarque 1.1.13 (2). du fait que celui-ci est défini modulo l'inertie).

**Théorème 1.2.2.** Si $L/K$ est une extension non ramifiée alors $(x, L/K) = \Phi^{v(x)}$.

**Remarque 1.2.3.** Si, ci-dessus, on avait choisi la normalisation classique pour la définition de $(x, L/K)$ (i.e si on n'avait pas précomposé par $x \longrightarrow x^{-1}$ le morphisme $\theta_{L/K}$) alors on aurait obtenu $(x, L/K) = F^{v(x)}$ où $F : y \longrightarrow y^{q_K}$ est le Frobenius classique.

**Corollaire 1.2.4.** $\forall x \in K^\times$, $\pi^{ab}(\theta_K(x)) = v(x)$ comme élément de $\hat{\mathbb{Z}}$.

**Lemme 1.2.5.** Le morphisme $\mathcal{W}_K^{ab} \longrightarrow G_K^{ab}$, induit par $\mathcal{W}_K \longrightarrow G_K$, est bijectif (où on a noté $G_K$ pour $Gal(\bar{K}/K)$).

On en déduit la suite exacte suivante :

$$0 \longrightarrow G_{K^{ab}/K_{nr}} \longrightarrow \mathcal{W}_K^{ab} \xrightarrow{\pi^{ab}} \mathbb{Z} \longrightarrow 0.$$

On peut rassembler toutes ces informations dans le diagramme suivant :

$$(3) \qquad \begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow \theta_K & & \downarrow \theta_K & & \downarrow Id & & \\ 1 & \longrightarrow & G_{K^{ab}/K_{nr}} & \longrightarrow & \mathcal{W}_K^{ab} & \xrightarrow{\pi^{ab}} & \mathbb{Z} & \longrightarrow & 1 \end{array}$$

On rappelle enfin, sous sa forme classique, le théorème principal de la théorie du corps de classes local :

**Théorème 1.2.6.** L'application $L \longrightarrow N_{L/K}(L^\times)$ est une bijection entre l'ensemble des extensions abéliennes finies de $K$ et les sous-groupes ouverts d'indice fini de $K^\times$.

**Démonstration.** Voir le théorème 1.4 p.321 de [41]. ■

On peut le reformuler en terme du groupe de Weil :

**Corollaire 1.2.7.** L'application de réciprocité $\theta_K$ est un isomorphisme (topologique) de $K^\times$ dans $\mathcal{W}_K^{ab}$.

**Démonstration.** Si $L/K$ est une extension finie abélienne dans $K^{ab}$, alors le théorème 1.2.6 montre que $\theta_K$ composé avec la projection $G_K^{ab} \twoheadrightarrow G_{L/K}$ envoie $K^\times$ surjectivement sur $G_{L/K}$. En laissant $L$ varier, on voit que $\theta_K$ envoie $K^\times$ sur un sous-groupe dense de $G_K^{ab}$. Comme $\mathcal{O}_K^\times$ est compact, on déduit du diagramme (3) que $\theta_K$ envoie $\mathcal{O}_K^\times$ sur $G_{K^{ab}/K_{nr}}$ puis que $\theta_K$ envoie $K^\times$ surjectivement sur $\mathcal{W}_K^{ab}$. Le noyau de $\theta_K$ est $\bigcap_{L/K \text{ finie ab}} N_{L/K}(L^\times)$. Si $i$ et $j$ sont des entiers $\geq 0$, alors $\left\{(\varpi_K^i)^n(1+\mathcal{O}_K^j)\,|n \in \mathbb{Z}\right\}$ est sous-groupe ouvert de

$K^\times$ d'indice fini et $\bigcap\limits_{i,j}\left\{(\varpi_K^i)^n(1+\mathcal{O}_K^j)\,|n\in\mathbb{Z}\right\}=\{1\}$. Or d'après le théorème 1.2.6, il existe une extension abélienne finie $L/K$ telle que $\left\{(\varpi_K^i)^n(1+\mathcal{O}_K^j)\,|n\in\mathbb{Z}\right\}=N_{L/K}(L^\times)$ On en déduit que :

$$\bigcap_{L/K \text{ finie ab}} N_{L/K}(L^\times)\subset\bigcap_{i,j}\left\{(\varpi_K^i)^n(1+\mathcal{O}_K^j)\,|n\in\mathbb{Z}\right\}=\{1\}$$

et donc $\theta_K$ est bijectif. Ainsi $\theta_K$ est un isomorphisme de groupe. ■

**Théorème 1.2.8.** L'isomorphisme $\theta_K$ identifie $U_K^{(n)}$ (le $n$-ième groupe des unités) avec $G^n(K^{ab}/K)$ (le $n$-ième groupe de ramification).

**Démonstration.** Voir le théorème 6.2 p.354 de [41]. ■

**Remarque 1.2.9.** Dans l'identification entre $K^\times$ dans $\mathcal{W}_K^{ab}$ :

$$\begin{array}{ccc} K^\times & \simeq & \mathcal{W}_K^{ab} \\ \varpi_K & \longleftrightarrow & \Phi \\ -1 & \longleftrightarrow & \alpha \end{array}$$

où $\Phi$ est le Frobenius (géométrique) et $\alpha$ l'unique élément de $I^{ab}$ d'ordre 2.

### 1.2.2 Symbole de Hilbert

On rappelle très rapidement la définition du symbole de Hilbert et ses principales propriétés. Le symbole de Hilbert $(,)_2$ apparaitra au chapitre 5.

Soit $K$ un corps local tel que $\mu_n\subset K$ (où $\mu_n$ désigne le groupe des racines $n$-ièmes de l'unité) et $L=K(\sqrt[n]{K^*})$ l'extension galoisienne abélienne maximale d'exposant $n$. D'après la théorie du corps de classes local on a :

$$Gal(L/K)\simeq K^\times/K^{\times n}$$

et par ailleurs (d'après la théorie de Kummer) :

$$Hom(Gal(L/K),\mu_n)\simeq K^\times/K^{\times n}.$$

L'application bilinéaire

$$\begin{array}{ccc} Gal(L/K)\times Hom(Gal(L/K),\mu_n) & \longrightarrow & \mu_n \\ (\sigma,\chi) & \to & \chi(\sigma) \end{array}$$

donne donc lieu à une application bilinéaire non-dégénérée :

$$(,)_n : K^\times/K^{\times n}\times K^\times/K^{\times n}\longrightarrow\mu_n$$

appellée le symbole de Hilbert.

**Proposition 1.2.10.** Le symbole de Hilbert vérifie les propriétés suivantes :

1. $(aa',b)_n=(a,b)_n(a',b)_n$ et $(a,bb')_n=(a,b)_n(a,b')_n$.
2. $(a,b)_n\Longleftrightarrow$ a est une norme d'un élément de $K(\sqrt[n]{b})$.
3. $(a,b)_n=(b,a)_n^{-1}$ (en particulier si $n=2$, $(a,b)_2=(b,a)_2$).
4. $(a,1-a)_n=1$, $(a,-a)_n=1$ et $(a,a)_n=(a,-1)_n$.
5. Si $(a,b)_n=1$ pour tout $b\in K^*$ alors $a\in K^{*n}$.

**Démonstration.** Voir la proposition 3.2 p.334 de [41]. ■

## 1.3 Groupes de Weil et Weil-Deligne et leurs représentations

On suit dans cette partie la très belle exposition de Rohrlich dans [45].

### 1.3.1 Représentations complexes du groupe de Weil

**Définition 1.3.1** (Représentations de $\mathcal{W}_K = \mathcal{W}(\bar{K}/K)$)**.** Une représentation de $\mathcal{W}_K$ est un morphisme *continu* $\sigma : \mathcal{W}_K \longrightarrow GL(V)$ où $V$ est $\mathbb{C}$-espace vectoriel de dimension finie.

**Proposition 1.3.2.** On a l'équivalence suivante :

1. $\sigma : \mathcal{W}_K \longrightarrow GL(V)$ est une représentation de $\mathcal{W}_K$.
2. $\sigma : \mathcal{W}_K \longrightarrow GL(V)$ est un morphisme tel que : $\sigma$ soit trivial sur un sous-groupe ouvert de $I_K$.
3. $\sigma : \mathcal{W}_K \longrightarrow GL(V)$ est un morphisme continu pour la topologie discrète de $GL(V)$.

On a $\mathcal{W}_K/\mathcal{W}_L = \mathcal{W}(\bar{K}/K)/\mathcal{W}(\bar{K}/L) = Gal(L/K)$.

Ainsi à une représentation $\theta$ de $Gal(L/K)$ on peut associer une représentation $\rho$ de $\mathcal{W}_K$ :

$$\rho : \mathcal{W}_K \twoheadrightarrow \mathcal{W}_K/\mathcal{W}_L = Gal(L/K) \xrightarrow{\theta} GL(V).$$

Ce sont précisément les représentations d'image finie de $\mathcal{W}_K$ (i.e $\sigma(\mathcal{W}_K)$ est un sous-groupe fini de $GL(V)$). On appelle ces représentations, les représentations de forme galoisienne de $\mathcal{W}_K$.

**Définition 1.3.3.** On définit la représentation de dimension 1, $\omega : \mathcal{W}_K \longrightarrow \mathbb{C}^\times$ par :
· $\omega$ est non-ramifié (i.e $\omega(I_K) = \{1\}$).
· $\omega(\Phi) = q^{-1}$ où $\Phi$ est un Frobenius géométrique (voir la remarque 1.1.13).

**Remarque 1.3.4.** Les représentations de $\mathcal{W}_K$ ne sont pas toutes semi-simples.
Par exemple, l'application $\rho : \mathcal{W}_K \longrightarrow GL_2(\mathbb{C})$ qui vérifie : $\begin{cases} \rho(I) = Id \\ \rho(\Phi) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{cases}$ est une représentation de $\mathcal{W}_K$ (ça se vérifie facilement grâce à la caractérisation 3. de la proposition 1.3.2) qui n'est pas semi-simple.

**Proposition 1.3.5** (Représentations irréductibles de $\mathcal{W}_K$)**.** Toutes représentations irréductibles de $\mathcal{W}_K$ est de la forme $\rho \otimes \omega^s$ où $\rho$ est une représentation de forme galoisienne de $\mathcal{W}_K$ et $s \in \mathbb{C}$.

**Démonstration.** Voir le corollaire 3 p.158 de [26] ou 4.10 p.542 de [11]. ■

**Corollaire 1.3.6** ("Théorème de Brauer")**.** Soit $\sigma$ une représentation du groupe de Weil. Alors on a :

$$[\sigma] = \sum_{(L,\chi)} c_{L,\chi}[Ind_{L/K}\chi]$$

où $[\sigma]$ est la classe de $\sigma$ dans le groupe de Grothendieck des représentations de $\mathcal{W}_K$, $(L, \chi)$ parcourt les paires telles que $L/K$ est une extension finie et $\chi$ un quasi-caractère de $\mathcal{W}(\bar{K}/L)$ et $c_{L,\chi}$ est un entier, nul pour presque tout $(L, \chi)$.

**Corollaire 1.3.7.** Soit $\sigma$ une représentation du groupe de Weil. Alors on a :

$$[\sigma] = (\dim \sigma)\,[1_K] + \sum_{(L,\chi,\chi')} c_{L,\chi,\chi'}[Ind_{L/K}(\chi - \chi')]$$

où $[\sigma]$ est la classe de $\sigma$ dans le groupe de Grothendieck des représentations de $\mathcal{W}(\bar{K}/K)$, $(L,\chi,\chi')$ parcourt les paires telles que $L/K$ est une extension finie et $\chi$ et $\chi'$ sont des quasi-caractères de $\mathcal{W}(\bar{K}/L)$ et $c_{L,\chi,\chi'}$ est un entier, nul pour presque tout $(L,\chi,\chi')$.

**Exemple 1.3.8 (Le cas d'une variété abélienne).** Soit $A$ une variété abélienne sur un corps $K$, on a une représentation $l$-adique naturelle de $Gal(\bar{K}/K)$ à travers son action sur le module de Tate :

$$\sigma : Gal(\bar{K}/K) \longrightarrow GL(T_l(A)) \text{ un morphisme continu.}$$

Le choix d'un plongement $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$ donne lieu à morphisme $\tilde{\sigma}$ de $\mathcal{W}(\bar{K}/K)$ dans $GL(T_l(A) \bigotimes_{\iota} \mathbb{C})$ :

$$\tilde{\sigma} : \mathcal{W}(\bar{K}/K) \longrightarrow GL(T_l(A) \bigotimes_{\iota} \mathbb{C}).$$

Si $\tilde{\sigma}$ est une représentation de $\mathcal{W}_K$ (i.e $\tilde{\sigma}$ est un morphisme continu) alors $\tilde{\sigma}$ est triviale sur un sous-groupe ouvert $J$ de $I$ (qui est donc d'indice fini dans $I$, car $I$ est compact). Ainsi l'action de $I$ sur $T_l(A)$ se factorise à travers un quotient fini $I/J$. D'après le critère de Néron-Ogg-Shafarevich (voir le théorème 2 p.496 de [57]) ceci n'est possible que si $A$ a potentiellement bonne réduction.
Ainsi si on veut pouvoir associer une représentation complexe à la représentation $l$-adique de $Gal(\bar{K}/K)$ associée à $A$ (même lorsque $A$ a réduction potentiellement multiplicative), il va falloir "grossir" un peu le groupe de Weil.

### 1.3.2 Groupe de Weil-Deligne et ses représentations

On a toujours $K$ une extension de $\mathbb{Q}_l$ et $k$ son corps résiduel avec $\#k = q$.

**Définition 1.3.9.** On définit le groupe de Weil-Deligne comme le produit semi-direct suivant :

$$\mathcal{WD}_K = \mathcal{WD}(\bar{K}/K) = \mathcal{W}(\bar{K}/K) \ltimes \mathbb{C}$$

où l'action est définie par : $\begin{array}{ccccc} \mathcal{W}_K \times \mathbb{C} & \longrightarrow & \mathbb{C} \\ (g,z) & \to & \omega(g)z \end{array}$ où $\omega$ est le caractère non-ramifié défini précédemment. On en fait un groupe topologique en le munissant de la topologie produit.

**Définition 1.3.10** (Représentation de $\mathcal{WD}_K$)**.** Une représentation de $\mathcal{WD}_K$ est un morphisme *continu* $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ où $V$ est $\mathbb{C}$-espace vectoriel de dimension finie.

**Proposition 1.3.11.** La donnée d'une représentation $\sigma'$ de $\mathcal{WD}_K$ est équivalente à la donnée d'un couple $(\sigma, N)$ où $\sigma$ est une représentation du groupe de Weil dans $V$ et $N$ est un endomorphisme de $V$.

$$\begin{array}{ccc} Rep_V(\mathcal{WD}_K) & \longleftrightarrow & \left\{ \begin{array}{c} (\sigma,N) \in Rep_V(\mathcal{W}_K) \times End_{Nil}(V) \\ \text{tel que } \sigma(g)N\sigma(g)^{-1} = \omega(g)N \end{array} \right\} \\ \sigma' & \longrightarrow & \left(\sigma'_{|\mathcal{W}_K}, \dfrac{\log \sigma'(z)}{z}\right) \\ gz \to \sigma(z)\exp(zN) & \longleftarrow & (\sigma, N) \end{array}$$

où $End_{Nil}(V)$ désigne les endomorphismes nilpotents de $V$ et $Rep_V(\mathcal{W}_K)$ (respectivement $Rep_V(\mathcal{WD}_K)$) les représentations $\sigma : \mathcal{W}_K \longrightarrow GL(V)$ (respectivement $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$)

**Démonstration.** Voir par exemple §3 de [45]. ■

**Remarque 1.3.12.**
1. Si $N \in End(V)$, la condition $\sigma(g)N\sigma(g)^{-1} = \omega(g)N$ entraine que $N \in End_{Nil}(V)$. En particulier, si $g = \Phi$ on obtient $\sigma(\Phi)N = q^{-1}N\sigma(\Phi)$ (ou encore $\sigma(\Phi)N\sigma(\Phi)^{-1} = q^{-1}N$).
2. Soit $\sigma' = (\sigma, N)$ et $\rho' = (\rho, M)$ alors :

$$\sigma' \simeq \rho' \Longleftrightarrow \sigma \overset{f}{\simeq} \rho \text{ et } f \circ N = M \circ f.$$

On peut se demander s'il existe des représentations "irréductibles" de $\mathcal{WD}_K$ qui donnent toutes les autres comme dans le cas des groupes finis ou des représentations semi-simples (on a vu dans la remarque 1.3.4 que déjà les représentations de $\mathcal{W}_K$ ne sont pas toutes semi-simples).

On va s'intéresser à un sous-ensemble de représentations : les représentations admissibles (c'est le cas notamment pour une représentation de $\mathcal{WD}_K$ associée à une courbe elliptique ou a une variété abélienne).

**Définition 1.3.13.** Une représentation $\sigma' = (\sigma, N)$ de $\mathcal{WD}_K$ sera dite admissible (parfois $\Phi$-semi-simple ou encore Frobenius-semi-simple) si $\sigma$ est une représentation semi-simple de $\mathcal{W}_K$.

**Remarque 1.3.14.** Il est équivalent de demander que $\sigma(\Phi)$ soit semi simple pour un $\Phi$ (ou pour tout $\Phi$). C'est ce qui donne lieu à la terminologie $\Phi$-semi-simple.

**Définition 1.3.15.** Une représentation $\sigma' = (\sigma, N)$ de $\mathcal{WD}_K$ est dite indécomposable si elle ne peut pas s'écrire comme somme directe de sous-représentations.

**Définition 1.3.16.** Une représentation est dite irréductible s'il elle est non nulle et n'admet pas de sous-représentation stricte.

**Remarque 1.3.17.** Dans le cas d'une représentation semi-simple (en particulier une représentation d'un groupe fini) : indécomposable $\Longleftrightarrow$ irréductible. Ici ce n'est pas le cas, on a bien sûr : irréductible $\Longrightarrow$ indécomposable mais pas le contraire.
On n'a même pas $\left.\begin{array}{c}\text{indécomposable}\\ \text{admissible}\end{array}\right\} \Longrightarrow$irréductible (admissible = $\Phi$-semi-simple $\neq$ semi-simple) (voir ci-dessous le cas de la représentation spécial $sp(n)$)
Dans ce cadre, les "briques" élémentaires des représentations sont les représentations indécomposables. On va voir qu'au prix d'une restriction aux représentations admissibles, on retrouve des théorèmes familiers.

**Définition 1.3.18** (La représentation spéciale)**.** Soit $(e_1, e_2, ..., e_n)$ la base canonique de $\mathbb{C}^n$. On définit $sp(n) = (\sigma, N)$ où :

$$\sigma(g) = \begin{pmatrix} \omega(g) & 0 & \cdots & 0 \\ 0 & \omega(g)^2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \omega(g)^n \end{pmatrix} \text{ et } N = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$

**Remarque 1.3.19.** Si $\pi \simeq (\pi, 0)$ est une représentation irréductible de $\mathcal{W}_K$ alors le représentation $\pi \bigotimes sp(n)$ est une représentation admissible et indécomposable de $\mathcal{WD}_K$ (mais pas irréductible). Deligne a montré qu'en fait toute représentation admissible et indécomposable de $\mathcal{WD}_K$ est de ce type.

**Proposition 1.3.20.** Toute représentation admissible et indécomposable de $\mathcal{WD}_K$ est de la forme $\pi \bigotimes sp(n)$ où $\pi \simeq (\pi, 0)$ est une représentation irréductible de $\mathcal{W}_K$.

**Démonstration.** Voir la proposition p.133 de [45]. ■

On en déduit un lemme de Schur pour ce type de représentation :

**Corollaire 1.3.21** ("Lemme de Schur")**.** Si $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ est une représentation admissible et indécomposable et si $T \in End(V)$ commute à l'action de $\mathcal{WD}_K$ :

$$\begin{array}{ccc} V & \xrightarrow{T} & V \\ \sigma'(g) \downarrow & & \downarrow \sigma'(g) \quad \text{est commutatif } \forall g \in \mathcal{WD}_K \\ V & \xrightarrow{T} & V \end{array}$$

alors

$$T = \lambda.Id \text{ avec } \lambda \in \mathbb{C}.$$

**Corollaire 1.3.22** (Décomposition en indécomposables)**.** Si $\sigma'$ est une représentation admissible de $\mathcal{WD}_K$ alors on a :

$$\sigma' = \bigoplus_{j=1}^{s} \pi_j \bigotimes sp(n_j)$$

où $\pi \simeq (\pi, 0)$ est une représentation irréductible de $\mathcal{W}_K$ et $n_j \in \mathbb{N}^*$.
De plus, si :

$$\sigma' = \bigoplus_{j=1}^{t} \rho_j \bigotimes sp(m_j)$$

est une autre telle décomposition alors : $s = t$ et quitte à renuméroter $\pi_j \simeq \rho_j$ et $m_j = n_j$.

### 1.3.3 Représentations $\mathfrak{p}$-adique du groupe de Galois absolu de $K$ et représentation complexe du groupe de Weil-Deligne

On rappelle que $K$ est toujours une extension finie de $\mathbb{Q}_l$. Soit $E$ un corps de nombres et $E_{\mathfrak{p}}$ le complété de $E$ en $\mathfrak{p}$ ($\mathfrak{p}$ une place au-dessus de $p$ et $p \neq l$).

**Définition 1.3.23.** Une représentation $\mathfrak{p}$-adique de $Gal(\bar{K}/K)$ est un morphisme continu :

$$\sigma'_{\mathfrak{p}} : Gal(\bar{K}/K) \longrightarrow GL(V_{\mathfrak{p}})$$

où $V_{\mathfrak{p}}$ est un $E_{\mathfrak{p}}$-espace vectoriel de dimension finie.

Commençons par donner la structure du groupe d'inertie modéré $I_K^{mr} = I_K/P_K$ (où $I_K$ est le groupe d'inertie et $P_K$ le pro-$l$-groupe d'inertie sauvage).

Si $\varpi$ est une uniformisante de $K_{nr}$ alors $K_{mr}$ (l'extension modérément ramifiée maximale) est le compositum des extensions $K_{nr}(\varpi^{1/n})$ où $n$ est premier à $l$ et :

$$I_K^{mr} = I_K/P_K \simeq \prod_{p \neq l} \mathbb{Z}_p.$$

Comme $P_K$ est un pro-$l$-groupe et que $p \neq l$, il existe un sous-groupe distingué fermé profini $Q$ de $I_K$ (d'ordre premier à $l$) tel que $I_K/Q \simeq \mathbb{Z}_p$ et :

**Lemme 1.3.24.** L'espace des morphismes continus de $I_K$ dans $\mathbb{Q}_p$ est de dimension 1 sur $\mathbb{Q}_p$.

On peut donc fixer un morphisme $t_p : I_K \longrightarrow \mathbb{Q}_p$ continu et non nul. On a alors que tout morphisme $f : I_K \longrightarrow \mathbb{Q}_p$ est la multiplication de $t_p$ par un élément de $\mathbb{Q}_p^\times$.

**Théorème 1.3.25.** Soit $\sigma_\mathfrak{p}$ une représentation $\mathfrak{p}$-adique de $Gal(\bar{K}/K)$ et $\iota : E_\mathfrak{p} \hookrightarrow \mathbb{C}$ une injection on a :

1. Il existe un unique endomorphisme nilpotent $N \in End(V_\mathfrak{p})$ et un sous groupe ouvert $J$ de $I_K$ tel que :
$$\forall i \in J,\ \sigma_\mathfrak{p}(i) = \exp(t_p(i)N)$$
2. Le morphisme $\sigma : \mathcal{W}_K \longrightarrow GL(V_\mathfrak{p})$ défini par :
$$\forall g \in \mathcal{W}_K,\ \sigma(g) = \sigma_\mathfrak{p}(g)\exp(-t_p(i)N)$$
où $i$ est tel que $g = \Phi^m i$, est une représentation de $\mathcal{W}_K$ et le couple $(\sigma, N)$ est une représentation de $\mathcal{WD}_K$.
3. Soit $(\sigma, N)$ une représentation de $\mathcal{WD}_K$ (comme en 2.). Pour chaque $g \in \mathcal{W}_K$, notons $\sigma^{ss}(g)$ la composante semi-simple dans la décomposition de Jordan multiplicative (appelée aussi décomposition de Dunford multiplicative) de $\sigma(g)$. L'application $g \longrightarrow \sigma^{ss}(g)$ est une représentation semi-simple de $\mathcal{W}_K$ triviale sur un sous-groupe ouvert de $I_K$ et $\boldsymbol{\sigma}^{ss}$=$(\sigma^{ss}, N)$ une représentation de $\mathcal{WD}_K$. Si on note $\sigma_\iota$ la représentation complexe de $\mathcal{W}_K$ obtenue par tensorisation par $\otimes_\iota\mathbb{C}$ et $N_\iota = N \otimes_\iota \mathbb{C} \in End(V_l \otimes_\iota \mathbb{C})$ alors $\sigma'_\iota = (\sigma_\iota, N_\iota)$ est une représentation complexe de $\mathcal{WD}_K$ qui ne dépend ni du choix de $\Phi$, ni de celui de $t_p$.

**Démonstration.** Ce théorème est dû à A. Grothendieck, voir la proposition p.131 de [45].

■

**Exemple 1.3.26** (**Le cas d'une variété abélienne**)**.** On a une représentation $p$-adique de $Gal(\bar{K}/K)$ canonique dans le module de Tate de la variété abélienne $A$ (de dimension $g$).
On rappelle que le module de Tate $T_p(A)$ est un $\mathbb{Z}_p$-module libre de rang $2g$ On notera $V_p(A) = T_p(A) \bigotimes \mathbb{Q}_p$.

L'action de $Gal(\bar{K}/K)$ sur les $A[p^n]$ est compatible avec le système projectif et on obtient par conséquent une action de $Gal(\bar{K}/K)$ sur $V_p(A)$ (et sur $V_p(A)^*$). On considérera généralement plutôt celle sur $V_p(A)^*$ :

$$\rho_p : Gal(\bar{K}/K) \longrightarrow GL(V_p(A)^*)$$

car $V_p(A)^* = H^1_p(A)$ et en fait dans la généralisation au cadre d'une courbe projective lisse $X$ on a une représentation de $Gal(\bar{K}/K)$ dans $H^1_p(X)$. On peut ensuite, selon la démarche explicitée dans la proposition précédente, lui associer une représentation complexe $\sigma'_{A/K,p,\iota} = (\sigma_{A/K,p,\iota}, N_{A/K,p,\iota})$ du groupe de Weil-Deligne. Cette représentation est indépendante du choix de $p$ et $\iota$ comme le montre la description explicite ci-dessous pour les courbes elliptiques.

Dans le cas où $A$ est une courbe elliptique, l'étude de cette représentation se décompose "naturellement" en deux sous-cas (notamment pour montrer que $\sigma'_{A/K,p,\iota}$ ne dépend ni de $p$ ni de $\iota$) :

1. La courbe a potentiellement bonne réduction.
   Dans ce cas, on montre que :
   (a) $N_{A/K,p,\iota} = 0$.
   (b) $\sigma_{A/K,p,\iota}$ est semi-simple (et par conséquent ne dépend pas du choix de $l$ et $\iota$, car Serre et Tate ont montré que $tr(\sigma_{A/K,p,\iota})$ est rationnel et indépendant de $p$).
   (c) $A$ a bonne réduction $\Leftrightarrow$ $\sigma_{A/K}$ est non ramifiée (c'est le critère de Néron-Ogg-Shafarevich).
2. La courbe a une réduction potentiellement multiplicative.
   Notons $A^\chi$ le twist de $A$ par $\chi$ tel que $A^\chi$ est réduction multiplicative scindée sur $K$ et $\chi^2 = 1$ (c'est possible voir notamment [58, Lemme 5.2 (c) p.440 et exercice 5.11 p.451]).
   On montre alors que :
   (a) $\sigma'_{A/K,p,\iota}$ est une représentation admissible et indécomposable.
   (b) $\sigma'_{A/K,p,\iota} = \chi\omega^{-1} \bigotimes sp(2)$ (qui est clairement indépendant de $p$ et de $\iota$) et donc $N_{A/K} \neq 0$.
      i. $\chi$ est trivial $\Leftrightarrow$ $A$ est réduction multiplicative déployée sur $K$.
      ii. $\chi$ est non-trivial et non ramifié $\Leftrightarrow$ $A$ est réduction multiplicative non déployée sur $K$.
      iii. $\chi$ est non-trivial et ramifié $\Leftrightarrow$ $A$ est réduction additive sur $K$.

## 1.4 Prémotifs et représentations du groupe de Weil-Deligne

Dans ce paragraphe, on change de notation : $K$ désigne un corps de nombres et $v$ une place finie de $K$. On note $K_v$ le complété de $K$ en $v$, $\mathcal{O}_{K_v}$ son anneau des entiers et $q_v = l_v^d$ le cardinal de son corps résiduel.

Soit $E$ un corps de nombres et $E_\mathfrak{p}$ le complété de $E$ en $\mathfrak{p}$ ($\mathfrak{p} \mid p$). On note $\mathcal{O}_{E_\mathfrak{p}}$ son anneau des entiers.

**Définition 1.4.1.**
1. Une représentation $\mathfrak{p}$-adique de dimension $n$ de $Gal(\overline{K}/K) = G_K$ est un morphisme continu de $G_K$ dans $GL_n(E_\mathfrak{p})$.
2. Une famille $\{\sigma_\mathfrak{p}\}$ de représentations $\mathfrak{p}$-adiques de $Gal(\overline{K}/K)$ est une famille de représentations (de même dimension) telle que pour chaque place $\mathfrak{p}$ de $E$, $\sigma_\mathfrak{p}$ est une représentation $\mathfrak{p}$-adique.

**Définition 1.4.2.** Une famille $\{\sigma_\mathfrak{p}\}$ de représentations $\mathfrak{p}$-adiques de $G_K$ est dite *complètement compatible* si elle vérifie les deux conditions suivantes :

1. Il existe un ensemble fini $S$ de places de $K$, indépendant de $\mathfrak{p}$, tel que $\sigma_\mathfrak{p}$ est non ramifiée en dehors de $S \cup \{w \mid w \text{ divise } p\}$ ($p$ est la caractéristique résiduelle de $E_\mathfrak{p}$).
2. Si on fixe une place (finie) $\mathfrak{q}$ de $K$ tel que $\mathfrak{q} \nmid p$ alors le polynôme $B_\mathfrak{q}(x) = \det(1 - x\sigma_\mathfrak{p}(\Phi_\mathfrak{q}) \mid V_\mathfrak{p}^I)$ (où $\Phi_\mathfrak{q}$ est un Frobenius géométrique en $\mathfrak{q}$) est à coefficients dans $E$ et est indépendant de $\mathfrak{p}$ (autrement dit, si $\mathfrak{p}' \mid p'$ est une autre place de $E$ telle que $\mathfrak{q} \nmid p'$ alors $\det(1 - x\sigma_\mathfrak{p}(\Phi_\mathfrak{q}) \mid V_\mathfrak{p}^I) = \det(1 - x\sigma_{\mathfrak{p}'}(\Phi) \mid V_{\mathfrak{p}'}^I)$.

**Remarque 1.4.3.** Le terme "complètement compatible" n'est pas standard dans la littérature, c'est ce que Rohrlich appelle "fully compatible" dans [48].

Si $\sigma$ est une représentation de $G_K$ et $v$ est une place de $K$ alors si on choisit une place de $\overline{K}$ au-dessus de $v$, on peut identifier le sous-groupe de décomposition correspondant avec $G_{K_v}$ et la classe d'isomorphie de la représentation $\sigma\,|G_{K_v}$ de $G_{K_v}$ est indépendante du choix de la place de $\overline{K}$ au-dessus de $v$.

**Définition 1.4.4.** On appellera famille faiblement compatible (et on notera $M$) une famille $\{\sigma_{\mathfrak{p}}\}$ de représentations $\mathfrak{p}$-adiques *complètement compatible* de $G_K$ qui vérifie de plus la condition suivante :
Si $v$ est une place de $K$ alors $\forall g \in Gal(\overline{K}_v/K_v) = G_{K_v}$ tel que son image dans $G_{K_v}/I_v$ soit une puissance entière du Frobenius alors le polynôme caractéristique de $\sigma_{\mathfrak{p}}(g)$ est à coefficients dans $E$ et est indépendant de $\mathfrak{p}$ pour toute place $\mathfrak{p}$ tel que $\mathfrak{p} \nmid l_v$.

**Remarque 1.4.5.** La famille de représentations issue d'une variété abélienne à travers ses modules de Tate forment une famille faiblement compatible (dans ce cas le corps $E$ est simplement le corps $\mathbb{Q}$). Voir notamment [45] pour le cas des courbes elliptiques, le théorème 3 p.499 de [57] pour le cas des variétés abéliennes de potentiellement bonne réduction et le théorème 4.3 p.41 de l'exposé IX de [25] pour les variétés abéliennes dans le cas général.

Si on part d'une famille faiblement compatible $M$ (avec les notations ci-dessus), si la caractéristique résiduelle $l_{\mathfrak{p}}$ de $E_{\mathfrak{p}}$ est différente de la caractéristique résiduelle $l_v$ de $K_v$, alors (d'après le théorème 1.3.25) la représentation $\sigma_{\mathfrak{p},v} = \sigma_{\mathfrak{p}}\,|G_{K_v}$ donne lieu à une représentation $\boldsymbol{\sigma} = (\sigma, N)$ de $\mathcal{WD}_{K_v}$ sur $E_{\mathfrak{p}}$ et par suite à la représentation $\boldsymbol{\sigma}^{ss} = (\sigma^{ss}, N)$ de $\mathcal{WD}_{K_v}$ sur $E_{\mathfrak{p}}$. Pour obtenir une représentation sur $\mathbb{C}$, il suffit de fixer un plongement $\iota_{\mathfrak{p}}$ de $E_{\mathfrak{p}}$ dans $\mathbb{C}$. Comme on voit $E$ comme un sous-corps de $E_{\mathfrak{p}}$, on peut demander que $\iota_{\mathfrak{p}}$ fixe $E$ (où $E$ est identifié à un sous-corps de $\mathbb{C}$ par un plongement $\iota$). En étendant les scalaires de $E_{\mathfrak{p}}$ à $\mathbb{C}$ on obtient une représentation $((\sigma^{ss})^{\iota_{\mathfrak{p}}}, N^{\iota_{\mathfrak{p}}})$ de $\mathcal{WD}_{K_v}$ sur $\mathbb{C}$. Il semble alors naturel de poser $\sigma_{\iota M,v} := ((\sigma^{ss})^{\iota_{\mathfrak{p}}}, N^{\iota_{\mathfrak{p}}})$.

**Définition 1.4.6.** On appellera prémotif (ou famille fortement compatible), une famille faiblement compatible telle que, pour tout $v$, la classe d'isomorphie de $\sigma_{\iota M,v}$ est indépendante des choix de $\mathfrak{p}$ et $\iota_{\mathfrak{p}}$.

**Remarque 1.4.7.**

1. Il serait agréable de savoir que toute famille faiblement compatible est fortement compatible (i.e est un prémotif). D'importants résultats dans ce sens ont été démontrés par T.Barnet-Lamb, T.Gee, D.Geraghty et R.Taylor sur des corps totalement réel ou CM (voir le théorème 5.4.3 de [2]).
2. La famille faiblement compatible associée à une courbe elliptique est un prémotif grâce à la description explicite (voir 1.3.26) de $((\sigma^{ss})^{\iota_{\mathfrak{p}}}, N^{\iota_{\mathfrak{p}}})$ dans ce cas.
3. Plus généralement, la famille faiblement compatible associée à une variété abélienne est un prémotif grâce à la description explicite (voir la proposition 1.10 de [51]) de $((\sigma^{ss})^{\iota_{\mathfrak{p}}}, N^{\iota_{\mathfrak{p}}})$ dans ce cas.

# Chapitre 2

# Fonctions $L$, facteurs epsilon et signes locaux

On rappelle tout d'abord quelques définitions et propriétés des représentations compatibles avec un accouplement notamment celles qu'on appellera (essentiellement) symplectique et orthogonale qui seront centrales dans nos considérations futures et dont les signes locaux (root numbers en anglais) vérifient des propriétés particulières.

## 2.1 Représentations compatibles avec un accouplement

Soit $K$ une extension finie de $\mathbb{Q}_l$.

**Définition 2.1.1.** Soit $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ une représentation complexe. Par une forme $\sigma'$-invariante, on entend une application bilinéaire ou sesquilinéaire $\langle , \rangle$ sur $V$ tel que :

1. $\langle , \rangle$ est non dégénérée.
2. $\langle , \rangle$ est stable par $\sigma'$ (ie : $\langle \sigma'(g)v, \sigma'(g)w \rangle = \langle v, w \rangle \ \forall g \in \mathcal{WD}_K$).

**Remarque 2.1.2.** On a $\langle \sigma'(g)v, \sigma'(g)w \rangle = \langle v, w \rangle \ \forall g \in \mathcal{WD}_K$
$$\iff \begin{cases} \langle \sigma(g)v, \sigma(g)w \rangle = \langle v, w \rangle \ \forall g \in \mathcal{W}(\bar{K}/K) \\ \langle Nv, w \rangle = - \langle v, Nw \rangle \end{cases}$$

**Définition 2.1.3.** Soit $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ une représentation complexe. On dira que :

1. $\sigma'$ est unitaire si $\exists \langle , \rangle$ une forme $\sigma'$-invariante qui est hermitienne.
2. $\sigma'$ est orthogonale si $\exists \langle , \rangle$ une forme $\sigma'$-invariante qui est symétrique.
3. $\sigma'$ est symplectique si $\exists \langle , \rangle$ une forme $\sigma'$-invariante qui est symplectique.
4. $\sigma'$ est essentiellement unitaire de poids $t \in \mathbb{R}$ si $\sigma' \bigotimes \omega^{t/2}$ est unitaire.
5. $\sigma'$ est essentiellement orthogonale de poids $t \in \mathbb{R}$ si $\sigma' \bigotimes \omega^{t/2}$ est orthogonale.
6. $\sigma'$ est essentiellement symplectique de poids $t \in \mathbb{R}$ si $\sigma' \bigotimes \omega^{t/2}$ est symplectique.

Là encore on retrouve un résultat familier, le théorème de Frobenius-Schur (voir [54] Théorème.31 p.121), en regardant simplement les représentations admissibles.

**Proposition 2.1.4.** Soit $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ une représentation admissible et indécomposable. On a alors :

1. La représentation $\sigma'$ est essentiellement unitaire.

2. La représentation $\sigma'$ est essentiellement orthogonale ou essentiellement symplectique si et seulement si $tr(\sigma')$ est à valeur réelle (i.e $\chi_{\sigma'}$ est à valeur réelle).

**Démonstration.** Voir la proposition p.136 de [45]. ■

**Exemple 2.1.5** (Le cas d'une variété abélienne)**.** On s'est donné une représentation $\sigma'_{A/K}$ provenant de $\rho_p : Gal(\bar{K}/K) \longrightarrow GL(V_p(A)^*)$. Si $A^t$ est la variété abélienne duale de $A$, on a l'accouplement de Weil :

$$\langle , \rangle : T_l(A) \times T_l(A^t) \longrightarrow T_l(\mu) \text{ où } T_l(\mu) = \varprojlim_n \mu_{l^n}$$

qui donne (dès lors qu'on se fixe une polarisation de $A$ dans sa duale $A^t$ qui donne lieu à une injection de $T_l(A)$ dans $T_l(A^t)$ à conoyau fini) une forme symplectique équivariante par $Gal(\bar{K}/K)$ sur $T_l(A)$ :

$$\langle , \rangle : T_l(A) \times T_l(A) \longrightarrow T_l(\mu).$$

En tant que $Gal(\bar{K}/K)$-module, $T_l(\mu) \simeq \mathbb{Z}_l \bigotimes \omega_l$ où $\omega_l : Gal(\bar{K}/K) \longrightarrow \mathbb{Z}_l^*$ est le caractère cyclotomique $l$-adique.

$$\begin{array}{ccccc} Gal(\bar{K}/K) & \underset{\rightarrow}{\longrightarrow} & U_{l^n} & \underset{\rightarrow}{\simeq} & (\mathbb{Z}/l^n\mathbb{Z})^* \\ \underset{g}{\downarrow} & & \underset{\chi_l(\xi_n)=\xi_n^{a_{g,n}}}{\downarrow} & & \underset{a_{g,n}}{\downarrow} \\ Gal(\bar{K}/K) & \underset{\rightarrow}{\longrightarrow} & U_{l^m} & \underset{\rightarrow}{\simeq} & (\mathbb{Z}/l^m\mathbb{Z})^* \\ \underset{g}{} & & \underset{\chi_l(\xi_m)=\xi_m^{a_{g,m}}}{} & & \underset{a_{g,m}}{} \end{array}$$

les $a_{g,n}$ sont compatibles et par passage à la limite projective on obtient :

$$\begin{array}{rccc} \omega_l : & Gal(\bar{K}/K) & \longrightarrow & \mathbb{Z}_l^* \\ & g & \rightarrow & a_g \end{array}$$

(c'est aussi l'unique caractère $l$-adique tel que $(\omega_l)_{|\mathcal{W}(\bar{K}/K)} = \omega$).
Autrement dit :$\langle g.v, g.w\rangle = g.\langle v, w\rangle$ ($ie : \langle \rho_l(g)v, \rho_l(g)w\rangle = \omega_l(g)\langle v, w\rangle$).
Après extension des scalaires par $\mathbb{Q}_l$ et passage au dual, on obtient :

$$\langle , \rangle : V_l(A)^* \times V_l(A)^* \longrightarrow \mathbb{Z}_l \bigotimes \omega_l^{-1}$$

et la condition de $Gal(\bar{K}/K)$-équivariance devient :

$$\begin{array}{rl} & \left\langle \sigma'_{A/K,l}(g)v, \sigma'_{A/K,l}(g)w \right\rangle = \omega_l(g)^{-1}\langle v, w\rangle \\ \iff & \begin{cases} \left\langle \sigma_{A/K,l}(g)v, \sigma_{A/K,l}(g)w \right\rangle = \omega(g)^{-1}\langle v, w\rangle \ \forall g \in \mathcal{W}(\bar{K}/K) \\ \left\langle N_{A/K,l}v, w \right\rangle = -\left\langle v, N_{A/K,l}w \right\rangle \end{cases} \\ \implies & \left\langle \sigma'_{A/K,l,\iota}(g)v, \sigma'_{A/K,l,\iota}(g)w \right\rangle = \omega(g)^{-1}\langle v, w\rangle \end{array}$$

et donc $\left\langle \sigma'_{A/K} \bigotimes \omega^{1/2}(g)v, \sigma'_{A/K} \bigotimes \omega^{1/2}(g)w \right\rangle = \langle v, w\rangle$ ie $\sigma'_{A/K} \bigotimes \omega^{1/2}$ est symplectique. Ainsi $\sigma'_{A/K}$ est essentiellement symplectique de poids 1.

## 2.2 Fonctions L

On va maintenant regarder comment associer une fonction $L$ à une représentation du groupe de Weil-Deligne.
On va construire ces fonctions $L$ de façon similaire à la construction des fonctions $L$ d'Artin.

### 2.2.1 Les fonctions $L$ globales historiques

Depuis le début de ce chapitre, on considère des corps locaux. On fait ici un petit aparté globale pour motiver la définition locale des fonctions $L$ pour des représentations du groupe de Weil et de Weil-Deligne.

#### La fonction Zeta de Riemann

C'est la fonction $L$ "originale" :

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_{p \text{ premier}} \frac{1}{1-p^{-s}} \text{ défini pour } \mathrm{Re}(s) > 1.$$

Si on pose $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ et $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$ alors on appelle fonction Zeta de Riemann "complète" la fonction $Z(s) = \Gamma_{\mathbb{R}}(s)\zeta(s)$, on a alors le fameux théorème suivant :

**Théorème 2.2.1.** La fonction $Z(s)$ admet un prolongement holomorphe sur $\mathbb{C}\backslash\{0,1\}$ avec des pôles simples en 0 et 1 de résidus respectif $-1$ et 1 et satisfait l'équation fonctionnelle :

$$Z(s) = Z(1-s)$$

**Démonstration.** Voir par exemple le théorème 1.6 p.425 de [41]. ■

On mentionne, en passant, la fameuse conjecture suivante :

**Conjecture 2.2.2** (Hypothèse de Riemann)**.** Les zéros non triviaux de $Z(s)$ sont sur la droite $\mathrm{Re}(s) = 1/2$.

#### Les fonctions $L$ de Dirichlet

Une première généralisation de la fonction Zeta est la suivante :

Soit $\chi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ un caractère (de Dirichlet), alors on peut définir la fonction multiplicative $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ par $\chi(n) = \begin{cases} \chi(n) & \text{si } \mathrm{pgcd}(m,n) = 1 \\ 0 & \text{sinon} \end{cases}$ et la fonction $L$ associée :

$$L(\chi, s) = \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ premier}} \frac{1}{1-\chi(p)p^{-s}}$$

En posant cette fois,

$$L_\infty(\chi, s) = m^{(s+a)/2}\Gamma_{\mathbb{R}}(s+a) = \left(\frac{m}{\pi}\right)^{(s+a)/2} \Gamma\left(\frac{s+a}{2}\right)$$

où $a = \begin{cases} 0 & \text{si } \chi(-1) = 1 \\ 1 & \text{si } \chi(-1) = -1 \end{cases}$ et $\Lambda(\chi, s) = L(\chi, s)L_\infty(\chi, s)$. Si $\chi$ est un caractère de Dirichlet alors si pour tout $m' \mid m$, $\chi$ ne se factorise pas par $(\mathbb{Z}/m'\mathbb{Z})^*$ (ceci revient à dire que le conducteur de $\chi$ est strictement supérieur à 1) alors on dit que $\chi$ est primitif. On a alors de nouveau :

**Théorème 2.2.3.** Si $\chi$ est un caractère primitif non trivial alors $\Lambda(\chi, s)$ admet un prolongement holomorphe sur $\mathbb{C}$ et vérifie l'équation fonctionnelle :

$$\Lambda(\chi, s) = W(\chi)\Lambda(\bar{\chi}, 1-s)$$

où $W(\chi)$ est de valeur absolue 1.

**Démonstration.** Voir par exemple le théorème 2.8 p.440 de [41]. ■

**Les fonctions $L$ d'Artin.**

Dans l'exemple précédent, on peut voir $(\mathbb{Z}/m\mathbb{Z})^*$ comme le groupe de Galois de l'extension $\mathbb{Q}(\mu_m)/\mathbb{Q}$ à travers l'isomorphisme $\begin{array}{ccc}(\mathbb{Z}/m\mathbb{Z})^* & \simeq & Gal(\mathbb{Q}(\mu_m)/\mathbb{Q}) \\ p & \to & \varphi_p\end{array}$ et ainsi voir le caractère de Dirichlet $\chi$ comme une représentation de dimension 1 de $Gal(\mathbb{Q}(\mu_m)/\mathbb{Q})$. On a alors $L(\chi,s)=\prod_p \frac{1}{1-\chi(\varphi_p)p^{-s}}$. Il est alors naturel de se demander, si on ne pourrait pas associer une fonction $L$ à toute représentation d'un groupe de Galois de façon à généraliser le cas des caractère de Dirichlet.

Artin a apporté une réponse. Soit $K$ un corps de nombres, $L/K$ une extension galoisienne finie et $\rho : Gal(L/K) \longrightarrow GL(V)$ une représentation. On pose :

$$L(\rho,s)=\prod_{\mathfrak{p}\text{ premier}} \frac{1}{\det(1-\rho(\varphi_\beta)\mathcal{N}(\mathfrak{p})^{-s}\,|V^{I_\beta})}$$

où $\beta$ est un idéal premier de $L$ au-dessus de $\mathfrak{p}$ et $\mathcal{N} := N_{K/\mathbb{Q}}$. Comme dans les deux exemples précédents la fonction $L$ est produit de fonctions $L$ locales aux places finies $\frac{1}{\det(1-\rho(\varphi_\beta)\mathcal{N}(\mathfrak{p})^{-s}\,|V^{I_\beta})}$. On peut encore définir la fonction $L$ généralisée $\Lambda$ en incluant les places infinies ( les termes sont plus compliqués à définir) et on a à nouveau :

**Théorème 2.2.4.** $\Lambda(\chi,s)$ admet un prolongement méromorphe sur $\mathbb{C}$ et vérifie l'équation fonctionnelle :

$$\Lambda(\rho,s)=W(\rho)\Lambda(\bar{\rho},1-s)$$

où $W(\rho)$ est de valeur absolue 1.

**Démonstration.** Voir par exemple le théorème 12.6 p.540 de [41]. ■

### 2.2.2 Les fonctions $L$ locales des représentations du groupe de Weil et de Weil-Deligne

On peut, au lieu de regarder simplement les représentations des extensions galoisiennes finies, regarder les représentations du groupe de Weil (on a vu que celles-ci contiennent en particuler les précédentes).

Soit $K$ un corps local non archimédien et $\sigma : \mathcal{W}_K \longrightarrow GL(V)$), on pose alors :

$$L(\sigma,s)=\frac{1}{\det(1-\sigma(\Phi)q^{-s}\,|V^I)}.$$

où $q=N(\mathfrak{m}_K)$ est le cardinal du corps résiduel de $K$ (i.e une puissance de $l$). Pour pouvoir traiter notamment les fonctions $L$ issues des prémotifs (on a vu par exemple que dans le cas d'une courbe elliptique, le groupe de Weil-Deligne est indispensable pour traiter la réduction potentiellement multiplicative), on va maintenant associer une fonction $L$ aux représentations du groupe de Weil-Deligne. On procède pour ça dans le même esprit mais en tenant compte de l'endomorphisme nilpotent $N$.

**Définition 2.2.5.** Soit $K$ un corps local non archimédien et $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ une repésentation du groupe de Weil-Deligne, on pose

$$L(\sigma',s)=\frac{1}{\det(1-\sigma(\Phi)q^{-s}\,|V_N^I)} \text{ où } V_N^I = V^I \cap \ker N$$

**Proposition 2.2.6** (Propriétés des fonctions $L$)**.** 1. Si $\sigma'$ et $\tau'$ sont deux représentations de $\mathcal{WD}_K$ alors :

$$L(\sigma' \bigoplus \tau', s) = L(\sigma', s)L(\tau', s).$$

2. Si $\rho'$ est une représentation de $\mathcal{WD}_L$ (où $L/K$ est une extension finie) alors :

$$L(Ind_{L/K}(\rho'), s) = L(\rho', s)$$

**Démonstration.** Voir par exemple le §8 de [45]. ■

**Remarque 2.2.7.** Pour les représentations admissibles, 1) permet de se ramener à l'étude des représentations admissibles indécomposables, autrement dit de la forme $\pi \bigotimes sp(n)$ où $\pi$ est une représentation irréductible de $\mathcal{W}_K$

**Proposition 2.2.8.** Soit $\sigma' = \pi \bigotimes sp(n)$ alors :

$$L(\sigma', s) = L(\pi, s + n - 1)$$

**Démonstration.** Voir par exemple la proposition p.138 de [45]. ■

**Remarque 2.2.9.** Ainsi l'étude des fonctions $L$ de représentations admissibles de $\mathcal{WD}_K$ se ramène à l'étude des fonctions $L$ de représentation irréductible de $\mathcal{W}_K$.

**Remarque 2.2.10.** Supposons maintenant donnée une représentation $l$-adique de $G_K$ (i.e $\sigma'_l : Gal(\bar{K}/K) \longrightarrow GL(V_l)$) et un plongement $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$, il y a deux façons naturelles de définir une fonction $L$ associée à $\sigma'_l$ et $\iota$. On peut poser

$$L(\sigma'_l, \iota, s) = \iota \left( \frac{1}{\det(1 - \sigma'_l(\Phi)q^{-s} \Big| (V_l)^I)} \right)$$

mais aussi

$$L(\sigma'_{l,\iota}, s)$$

où $\sigma'_{l,\iota}$ est la représentation de $\mathcal{W}'(\bar{K}/K)$ associée à la représentation $l$-adique $\sigma'_l$. Il s'avère que ces deux définitions coïncident :

$$L(\sigma'_l, \iota, s) = L(\sigma'_{l,\iota}, s)$$

**Remarque 2.2.11.** Si maintenant $K$ est un corps de nombres et qu'on dispose d'un prémotif $M$ sur $K$ alors on peut construire une fonction $L$ "complète" (globale) $\Lambda(M, s)$ associée à $M$ (comme produit des fonctions $L$ locales des divers groupes de Weil-Deligne, voir la section 2.5 pour la définition des fonctions $L$ locales aux places archimédiennes). On peut espérer obtenir (comme dans le cas des représentations d'Artin) un prolongement holomorphe et une equation fonctionnelle. On discutera de ces conjectures au chapitre suivant (voir la section 3.2.1).

**Exemple 2.2.12** (Le cas d'une variété abélienne)**.** Si $A/K$ est une variété abélienne, on pose :

$$L(A/K, s) = L(\sigma'_{A/K}, s)$$

On retrouve la définition classique de la fonction $L$ d'une courbe elliptique. Soit $E/K$ une courbe elliptique alors :

1. Si $E$ a bonne réduction alors :

$$L(E/K,s)=\frac{1}{1-aq^{-s}+q^{1-2s}} \text{ où } a=1-\left|\tilde{E}(k)\right|+q$$

2. Si $E$ a réduction multiplicative déployée alors :

$$L(E/K,s)=\frac{1}{1-q^{-s}}$$

3. Si $E$ a réduction multiplicative non déployée alors :

$$L(E/K,s)=\frac{1}{1+q^{-s}}$$

4. Si $E$ a réduction additive alors :

$$L(E/K,s)=1$$

On pourra regarder [45] p.151 pour les détails.

## 2.3 Conducteurs

On énonce ici la définition de l'exposant du conducteur et on en donne une caractérisation qui servira de modèle à la définition des facteurs epsilon à la section suivante.

Soit $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ une représentation du groupe de Weil-Deligne, on va définir le conducteur de $\sigma'=(\sigma,N)$.

Soit $R/K^{nr}$ une extension galoisienne finie tel que $\sigma$ soit trivial sur $Gal(\bar{K}/R)\subset I$ (autrement dit, $R/K^{nr}$ contient tout la ramification de $\sigma$) et on pose :

$G_o=Gal(R/K^{nr})$ et $G_j=\{g\in G_0\,|v_R(\sigma(g)\varpi_R-\varpi_R)\geq j+1\}$. Les $G_j$ sont appelés les groupes de ramification supérieurs.

**Définition 2.3.1.** Soit $\sigma' : \mathcal{WD}_K \longrightarrow GL(V)$ une représentation du groupe de Weil-Deligne, on pose :

$$a(\sigma')=a(\sigma)+b(\sigma')$$

avec $a(\sigma)=\sum\limits_{j=0}^{\infty}\frac{|G_j|}{|G|}\dim(V/V^{G_j})$ et $b(\sigma')=\dim(V^I/V_N^I)$.
On appelle $a(\sigma')$ l'exposant du conducteur de $\sigma'$ et on définit le conducteur comme l'idéal de $\mathcal{O}_K$ suivant :

$$\mathcal{N}(\sigma')=\varpi_K^{a(\sigma')}\mathcal{O}_K$$

**Proposition 2.3.2** (Caractérisation de $a(\sigma)$)**.** L'exposant $a(\sigma)$ est entièrement déterminé par les 3 propriétés suivantes :

1. $a(*)$ est additif sur les suites exactes courtes.
2. Si $L/K$ est extension finie et $\rho : \mathcal{W}(\bar{K}/L)\longrightarrow GL(V)$ une représentation alors :

$$a(Ind_{L/K}\rho)=(\dim\rho)\,d(L/K)+f(L/K)a(\rho) \text{ où } Disc(L/K)=\varpi_K^{dL/K)}\mathcal{O}_K.$$

3. Si $\chi$ est un quasi-caractère de $L^\times$ (identifié à une représentation de dimension 1 de $\mathcal{W}(\bar{K}/L)$) alors :

$$a(\chi) = \begin{cases} 0 & \text{si } \chi \text{ est non ramifié,} \\ r_\chi & \text{si } \chi \text{ est ramifié,} \end{cases}$$

où $r_\chi$ le plus petit entier tel que $\chi$ est trivial sur $1 + \varpi_L^{r_\chi}\mathcal{O}_L$

**Démonstration.** Voir par exemple le théorème 1 p.107 et corollaire 2 p.108 de [53]. ■

**Remarque 2.3.3.**
1. Les termes de $a(\sigma)$ sont tous nuls sauf un nombre fini.
2. La définition est indépendante du choix de $R$.
3. On dit parfois que la fonction $a(*)$ est extensible (voir définition 2.4.3).

**Proposition 2.3.4.** Soient $\sigma'$, $\tau'$ et $\rho'$ des représentations du groupe de Weil-Deligne, on a :

1. $a(\sigma' \bigoplus \tau') = a(\sigma') \bigoplus a(\tau')$.
2. $a(Ind_{L/K}\rho') = (\dim \rho')\, d(L/K) + f(L/K)a(\rho')$.
3. Si $\dim \sigma' = 1$ et $\sigma' = (\sigma, 0)$ alors

$$a(\sigma') = a(\sigma) = \begin{cases} 0 & \text{si } \sigma \text{ est non ramifiée,} \\ \alpha & \text{si } \sigma \text{ est ramifiée,} \end{cases}$$

où $\alpha$ est le plus petit entier $m$ tel que $\sigma$ est trivial sur $1 + \varpi_L^m\mathcal{O}_L$.

**Proposition 2.3.5.** Soit $\sigma'$ une représentation admissible et indécomposable alors $\sigma' = \pi \bigotimes sp(n)$ et :

$$a(\sigma') = \begin{cases} n-1 \text{ si } \pi \text{ est non ramifiée} \\ na(\pi) \text{ si } \pi \text{ est ramifiée} \end{cases}$$

**Démonstration.** Voir par exemple la proposition p.141 de [45]. ■

**Exemple 2.3.6** (Le cas d'une courbe elliptique)**.** On définit comme pour les fonctions $L$, $a(E/K) = a(\sigma'_{E/K})$ et on a les résulats suivants :

1. Si $E/K$ a bonne réduction alors $a(E/K) = 0$.
2. Si $E/K$ a réduction multiplicative alors $a(E/K) = 1$.
3. Si $E/K$ a réduction additive alors :
   (a) Si $E/K$ a potentiellement bonne réduction et $p \geq 5$ alors $a(E/K) = 2$.
   (b) Si $E/K$ a potentiellement réduction multiplicative alors $a(E/K) = 2a(\chi)$ où $\chi$ est un caractère d'ordre 2 tel que $E^\chi/K$ a réduction multiplicative (cela ne dépend pas du choix de $\chi$).

On pourra regarder [45] p.152 pour les détails.

## 2.4 Facteurs epsilon et signes locaux

Sur le modèle des 3 propriétés définissant le conducteur $a(\sigma)$ d'une représentation du groupe de Weil, Deligne a défini des constantes $\varepsilon(*,*,*)$ qui dépendent de $\sigma$, d'un caractère additif $\psi : K \longrightarrow \mathbb{C}^*$ et d'une mesure de Haar $dx$ sur $K$.

Avant d'énoncer la proposition établissant l'existence de telles constantes $\varepsilon$, donnons deux définitions (contrairement au reste du chapitre dans ces deux définitions le corps $K$ peut aussi être global).

**Définition 2.4.1** ($(R(K)$ et $R_1(K))$)**.** On pose :

$$\begin{aligned} R(K) &= \left\{(L,\rho) \text{ où } \rho \text{ est une représentation de } Gal(\bar{K}/L)\right\} \\ \text{et} \quad R_1(K) &= \{(L,\chi) \text{ où } \chi : L^\times \longrightarrow \mathbb{C}^\times \text{ est caractère d'ordre fini}\} \end{aligned}$$

avec $K \subset L \subset \bar{K}$, $L/K$ une extension galoisienne finie et représentation signifie morphisme continu dans $GL_n(\mathbb{C})$.

**Remarque 2.4.2.** On peut identifier $R_1(K)$ à un sous-ensemble de $R(K)$ (grâce à la théorie du corps de classe).

**Définition 2.4.3** ((Extensibilité))**.** Une application $F : R_1(K) \longrightarrow A$ (où $A$ est un groupe abélien) est dite extensible si elle peut être prolongée en une application $\tilde{F} : R(K) \longrightarrow A$ telle que :

1. $F(L, \rho_1 + \rho_2) = F(L,\rho_1)F(L,\rho_2)$ pour tout $(L,\rho_1)\,,\,(L,\rho_2) \in R(K)$.
2. $F$ est stable par induction en degré 0, autrement dit :
   Si $K \subset L \subset L'$ et $\rho : Gal(\bar{K}/L) \longrightarrow GL(V)$ avec $\dim \rho = 0$ alors :

$$F(L,\rho) = F(L', Ind_{L/L'}(\rho)).$$

**Remarque 2.4.4.**
1. Pour la propriété 1, on peut demander simplement la propriété d'additivité sur les suites exactes (i.e linéarité dans le groupe de Grothendieck) et pas simplement sur les sommes directes, ce qui permet notamment que l'extensibilité fasse sens pour les représentations de $\mathcal{W}_K$ et de $\mathcal{WD}_K$.
2. Si $F$ est extensible alors le prolongement est unique.
3. Si $K \subset L \subset L'$ et $\rho : Gal(\bar{K}/L) \longrightarrow Gl(V)$ (où on a plus nécessairement $\dim \rho = 0$) alors :
$$F(L', Ind_{L/L'}(\rho)) = \lambda_{L/L'}(F)^{\dim \rho} F(L,\rho)$$
où $\lambda_{L/L'}(F) = \dfrac{F(L', Ind_{L/L'}(1_L))}{F(L,1_L)}$.

**Exemple 2.4.5.**
1. Extensibilité de $W(\cdot)$ sur un corps de nombres. Soit $K$ un corps de nombres :

$$\text{L'application } W : \begin{array}{ccc} R_1(K) & \longrightarrow & \mathbb{C}^\times \\ (L,\chi) & \to & W(\chi) \end{array} \quad \text{est extensible.}$$

   En effet, elle s'étend en $W : \begin{array}{ccc} R(K) & \longrightarrow & \mathbb{C}^\times \\ (L,\rho) & \to & \Lambda(\rho, 1-s)\Lambda(\bar{\rho}, s)^{-1} \end{array}$ d'après l'équation fonctionnelle des fonctions $L$ des représentations d'Artin (voir le théorème 2.2.4).

2. Si $c \in K^\times$ (cas local) ou $c$ est un élément du groupe des classes d'idèles (cas global). Alors l'application $\begin{array}{ccc} R_1(K) & \longrightarrow & \mathbb{C}^\times \\ (L,\chi) & \to & \chi(c) \end{array}$ est extensible. Son extension est donnée par :
$$\begin{array}{ccc} R(K) & \longrightarrow & \mathbb{C}^\times \\ (L,\rho) & \to & \det\rho(c) \end{array}.$$

3. Si $F : R_1(K) \longrightarrow \mathbb{C}^\times$ ne dépend que de $L$ (i.e $F(L,\chi) = a(L)$) alors $F$ est extensible d'extension $F(L,\rho) = a(L)^{\dim\rho}$.

On revient désormais au cas d'un corps local $K$ :

**Proposition 2.4.6.** Il existe une fonction $\varepsilon(*,*,*)$ vérifiant :

1. $\varepsilon(*,\psi,dx)$ est multiplicative sur les suites exactes courtes.
2. Soit $L/K$ une extension finie et $\rho : \mathcal{W}(\bar{K}/L) \longrightarrow GL(V)$ une représentation alors (pour toute mesure de Haar $dx_L$ sur $L$) :
$$\varepsilon(Ind_{L/K}\rho,\psi,dx) = \varepsilon(\rho,\psi\circ tr_{L/K},dx_L)\left(\frac{\varepsilon(Ind_{L/K}1_L,\psi,dx)}{\varepsilon(1_L,\psi\circ tr_{L/K},dx_L)}\right)^{\dim\rho}.$$
3. Si $\chi$ est un quasi-caractère de $L^\times$ (identifié à une rep de dimension 1 de $\mathcal{W}(\bar{K}/L)$) et $\psi_L$ un caractère additif de $L$ alors :
$$\varepsilon(\chi,\psi_L,dx_L) = \begin{cases} \chi\omega^{-1}(c)\int\limits_{\mathcal{O}_L} dx_L \text{ si } \chi \text{ est non ramifié,} \\ \int\limits_{c^{-1}\mathcal{O}_L^\times} \chi^{-1}(x)\psi_L(x)dx_L \text{ si } \chi \text{ est ramifié,} \end{cases}$$
où $c$ est un élément de $L^\times$ de valuation $n(\psi_L)+a(\chi)$ et $n(\psi_L)$ est le plus grand entier $m$ tel que $\psi_L$ est trivial sur $\pi_L^{-m}\mathcal{O}_L$.

**Remarque 2.4.7.** Les points 1. et 2. disent précisément que le facteur $\varepsilon(*,\psi,dx)$ défini par 3. est une fonction extensible.

**Démonstration (exquisse).** Pour plus de détails, on renvoie au théorème 4.1 de l'article de Deligne [11].

1. On traite le cas où $K$ est archimédien et on considère par la suite la cas non-archimédien.
2. On se ramène au cas des représentations d'Artin : On a vu (Proposition 1.3.5) que toute représentation irréductible $\sigma$ de $\mathcal{W}_K$ s'écrit de $\sigma = \rho\otimes\omega^s$ où $\rho$ est une représentation de $G_K$ (i.e une représentation d'Artin). On pose alors $\varepsilon(\sigma,\psi,dx) = \varepsilon(\rho,\psi,dx)$ et on définit alors $\varepsilon(*,\psi,dx)$ par additivité.
3. Le cas des représentations d'Artin :
   (a) D'après la thèse de Tate (voir [61]), il existe un facteur $\varepsilon(*,\psi,dx)$ pour les représentations de dimension 1 qui est défini comme le 3. de la proposition.
   (b) Passage par le cadre global : Si $\chi$ est un caractère d'ordre fini de $L^\times$ alors il existe une extension globale $l/k$, un caractère global $\tilde{\chi}$, une place $v_0$ de $k$ et une place $w_0$ de $l$ (la seule par construction de $l/k$) tel que $\chi = \tilde{\chi}_{w_0}$. on peut alors écrire $\varepsilon(\chi,\psi_{w_0},dx_{w_0}) = \varepsilon(\tilde{\chi}_{w_0},\psi_{w_0},dx_{w_0}) = \frac{\varepsilon(\tilde{\chi},\psi,dx)}{\prod\limits_{w\neq w_0}\varepsilon(\tilde{\chi}_w,\psi_w,dx_w)}$. Le point clef est

qu'en tensorisant par un caractère $\alpha$ bien choisi, on obtient $\varepsilon(\chi, \psi_{w_0}, dx_{w_0}) = \frac{\varepsilon(\tilde{\chi}\alpha,\psi,dx)}{\prod_{w\neq w_0}\varepsilon(\tilde{\chi}_w\alpha_w,\psi_w,dx_w)}$ tel que $\prod_{w\neq w_0}\varepsilon(\tilde{\chi}_w\alpha_w, \psi_w, dx_w)$ soit **extensible** (il s'exprime à l'aide de fonctions de la forme des points 2 et 3 de l'exemple 2.4.5). Par ailleurs, on sait que grâce à l'équation fonctionnelle globale pour les représentations d'Artin (global) que $\varepsilon(\tilde{\chi}\alpha, \psi, dx)$ est extensible (voir 1. de l'exemple 2.4.5). On en déduit l'existence de $\varepsilon(*, \psi, dx)$ pour les représentations d'Artin (locale).

4. On conclut à l'existence de $\varepsilon(*, *, *)$ pour les représentations du groupe de Weil (local).

■

Donnons tout de suite quelques propriétés de ce facteur epsilon.

**Proposition 2.4.8.** Pour $\alpha \in K^\times$, on note $\psi_\alpha$ le caractère $x \longrightarrow \psi(\alpha x)$.

1. $\varepsilon(\sigma, \psi_\alpha, dx) = (\det\sigma)(\alpha)\omega(\alpha)\varepsilon(\sigma, \psi, dx)$.
2. $\varepsilon(\sigma, \psi, rdx) = r^{\dim\sigma}\varepsilon(\sigma, \psi, dx)$.
3. $\varepsilon(\sigma \otimes \omega^s, \psi, dx) = \varepsilon(\sigma, \psi, dx)q^{-s(n(\psi)\dim(\sigma)+a(\sigma))}$ où $n(\psi)$ est l'entier défini dans la proposition 2.4.6.

Donnons maintenant la définition de $\varepsilon$ pour les représentations de $\mathcal{WD}_K$. :

**Définition 2.4.9.** Soit $\sigma' = (\sigma, N)$ une représentation de $\mathcal{WD}_K$, on pose :

$$\varepsilon(\sigma', \psi, dx) = \varepsilon(\sigma, \psi, dx)\delta(\sigma')$$

où $\varepsilon(\sigma, \psi, dx)$ est défini par la proposition précédente et $\delta(\sigma') = \det(-\sigma(\Phi)\Big|V^I/V_N^I)$.

**Proposition 2.4.10.** La fonction $\varepsilon$ définie sur $\mathcal{WD}_K$ vérifie les mêmes propriétés que la fonction $\varepsilon$ originale sur $\mathcal{W}_K$.

1. $\varepsilon(*, \psi, dx)$ est multiplicative sur les suites exactes courtes.
2. Soit $L/K$ une extension finie et $\sigma' : \mathcal{WD}(\bar{K}/L) \longrightarrow GL(V)$ une représentation alors ($\forall$ $dx_L$ mesure de Haar sur $L$) :

$$\varepsilon(Ind_{L/K}\sigma', \psi, dx) = \varepsilon(\sigma', \psi \circ tr_{L/K}, dx_L)\left(\frac{\varepsilon(Ind_{L/K}1_L, \psi, dx)}{\varepsilon(1_L, \psi \circ tr_{L/K}, dx_L)}\right)^{\dim\sigma'}.$$

3. Si $\sigma' = (\sigma, N)$ est de dimension 1 alors $\sigma' = (\sigma, 0)$ et $\varepsilon(\sigma', \psi, dx) = \varepsilon(\sigma, \psi, dx)$ où le second membre est défini comme au 3. de la proposition 2.4.6.

**Démonstration.** Voir les §11 et §12 de [45]. ■

**Définition 2.4.11.** On appelle signe local (ou "root number") le nombre complexe de module 1 suivant :

$$W(\sigma', \psi) = \frac{\varepsilon(\sigma', \psi, dx)}{|\varepsilon(\sigma', \psi, dx)|}$$

**Remarque 2.4.12.** Comme le suggère la notation, $W(\sigma', \psi)$ ne dépend pas de la mesure de Haar choisie. En effet, on peut montrer que :

$$\varepsilon(\sigma', \psi, rdx) = r^{\dim\sigma}\varepsilon(\sigma', \psi, dx)$$

et donc

$$\frac{\varepsilon(\sigma', \psi, dx)}{|\varepsilon(\sigma', \psi, dx)|} = \frac{\varepsilon(\sigma', \psi, rdx)}{|\varepsilon(\sigma', \psi, rdx)|}.$$

**Proposition 2.4.13.** (Propriétés de $\varepsilon(\sigma', \psi, dx)$ et $W(\sigma', \psi)$).
Soit $n(\psi)$ comme précédemment et $dx_\psi$ la mesure auto-duale relativement à $\psi$

1. $\varepsilon(\sigma, \psi, dx_\psi)\varepsilon(\sigma^*, \psi, dx_\psi) = (\det \sigma)(-1)q^{n(\psi)\dim(\sigma)+a(\sigma)}$.
2. $\delta(\sigma')\delta(\sigma'^*) = q^{b(\sigma')}$.
3. $\varepsilon(\sigma', \psi, dx_\psi)\varepsilon(\sigma'^*, \psi, dx_\psi) = (\det \sigma)(-1)q^{n(\psi)\dim(\sigma')+a(\sigma')}$.
4. Si $\sigma'$ est essentiellement orthogonale alors $W(\sigma', \psi) \in \{\pm 1, \pm i\}$.
5. Si $\sigma'$ est essentiellement symplectique alors $W(\sigma', \psi)$ ne dépend pas de $\psi$ et $W(\sigma') = \pm 1$.

**Démonstration.** Voir le lemme p.144 et la proposition p.145 de [45]. ∎

**Corollaire 2.4.14.** Soit $\sigma' = \pi \otimes sp(n)$ une représentation de $\mathcal{WD}_K$ où $\pi$ est une représentation irréductible de $\mathcal{W}_K$ et $n > 0$ un entier. Ecrivons $\pi = \rho \otimes \omega^{t+i\theta}$ où $\rho$ est une représentation d'Artin et $t, \theta \in \mathbb{R}$. Si $\pi$ est non-ramifié (donc de dimension 1), on pose $\chi = \rho\omega^{i\theta}$.

1. $|\varepsilon(\sigma', \psi, dx_\psi)| = q^{(-t+1-n/2)(n(\psi)\dim \sigma' + a(\sigma'))}$.
2. $\varepsilon(\sigma', \psi_{can}, dx_{can}) = W(\sigma', \psi)A(\sigma')^{-t+1-n/2}$ où $A(\sigma') = D_K^{\dim \sigma'} q^{a(\sigma')}$ où $D_K$ désigne le discriminant absolu de $K$.
3. $W(\sigma', \psi) = \begin{cases} W(\pi, \psi) & \text{si } \pi \text{ est ramifié,} \\ (-1)^{n-1}\chi(\Phi)^{n(n(\psi)+1)-1} & \text{si } \pi \text{ est non-ramifié.} \end{cases}$

**Démonstration.** Voir le corollaire p.146 de [45]. ∎

**Exemple 2.4.15** (Le cas d'une variété abélienne)**.** Soit $A/K$ une variété abélienne. On a vu que $\sigma'_{A/K}$ est essentiellement symplectique de poids 1 donc ne dépend pas du choix de $\psi$. Si on note $W(A/K) := W(\sigma'_{A/K})$ on a $W(E/K) = \pm 1$. Plus précisement, dans le cas où $A = E$ est une courbe elliptique on a :

1. Si $E/K$ a bonne réduction alors $W(E/K) = 1$.
2. Si $E/K$ a réduction multiplicative déployée alors $W(E/K) = -1$.
3. Si $E/K$ a réduction multiplicative non déployée alors $W(E/K) = 1$.
4. Si $E/K$ a réduction additive potentiellement multiplicative alors $(E/K) = \chi(-1)$ où $\chi$ est un caractère d'ordre 2 tel que $E^\chi$ ait réduction multiplicative déployée.
5. Si $E/K$ a potentiellement bonne réduction et $p > 3$. On note $\Delta \in K^\times$ le discriminant de $E$ et $e = \dfrac{12}{\gcd(ord_p\Delta, 12)}$ alors :

$$W(E/K) = \begin{cases} 1 & \text{si } 2 \mid f_{K/\mathbb{Q}_p} \text{ ou } e = 1, \\ \left(\dfrac{-1}{p}\right) & \text{si } 2 \nmid f_{K/\mathbb{Q}_p} \text{ et } e = 2 \text{ ou } 6, \\ \left(\dfrac{-3}{p}\right) & \text{si } 2 \nmid f_{K/\mathbb{Q}_p} \text{ et } e = 3, \\ \left(\dfrac{-2}{p}\right) & \text{si } 2 \nmid f_{K/\mathbb{Q}_p} \text{ et } e = 4. \end{cases}$$

On pourra regarder les articles [44] et [46] pour plus de détails.

On énonce enfin quelques résultats sur les facteurs epsilon qui nous serons utiles dans les chapitre 4 et 5.

On commence par une propriété de congruence due à Deligne (qui nous sera utile au chapitre 4).

**Définition 2.4.16.** On définit la constante $\varepsilon_0$ par :

$$\varepsilon(\sigma, \psi, dx) = \varepsilon_0(\sigma, \psi, dx) \det(-\sigma(\Phi) \Big| V^{I_K})^{-1}.$$

**Remarque 2.4.17.** Pour les propriétés de $\varepsilon_0$, on pourra consulter le §5 p.548 de [11].

**Proposition 2.4.18.** Soit $G$ un quotient fini de $\mathcal{W}_K$ et $L$ une extension finie de $\mathbb{Q}_p$ (avec $p \neq l$). On note $R_L(G)$ (resp $R_{k_L}(G)$) le groupe de Grothendieck de la catégorie des $L[G]$-module (resp $k_L[G]$-module) de type fini et $d : R_L(G) \longrightarrow R_{k_L}(G)$. Soient $\sigma_1$ et $\sigma_2$ deux représentations de $R_L(G)$ telles que $d(\sigma_1) = d(\sigma_2)$ alors :

$$\varepsilon_0(\sigma_1, \psi, dx) \equiv \varepsilon_0(\sigma_2, \psi, dx) \mod \varpi_L.$$

**Démonstration.** Voir [11] p.556-557. ■

Pour finir, donnons deux résultats connus concernant le comportement des facteurs epsilon (et donc des signes locaux) par torsion par une représentation (qui nous seront utiles aux chapitres 4 et 5) :

**Proposition 2.4.19.** Soit $\sigma$ une représentation de $\mathcal{WD}_K$. Si $\tau$ est une représentation non-ramifiée de $\mathcal{WD}_K$ alors :

$$\varepsilon(\sigma \otimes \tau, \psi, dx) = \varepsilon(\sigma, \psi, dx)^{\dim \tau} \det \tau \left( \varpi_K^{a(\sigma)+n(\psi)\dim \sigma} \right)$$

**Démonstration.** Voir le point (3.4.6) de [60] ou le corollaire 5 p.115 de [62]. ■

**Corollaire 2.4.20.** Soit $\sigma$ une représentation de $\mathcal{WD}_K$ alors pour tout $\alpha \in \mathbb{R}$, on a :

$$W(\sigma \otimes \omega^\alpha, \psi) = W(\sigma, \psi).$$

**Proposition 2.4.21.** Soit $\sigma$ une représentation modérément ramifiée de $\mathcal{WD}_K$. Si $\tau$ est une représentation totalement sauvagement ramifiée (c'est à dire une représentation dont aucun de ses constituants n'est modérément ramifié) alors il existe un élément $\gamma \in K^\times$ tel que :

$$\varepsilon(\sigma \otimes \tau, \psi, dx) = \varepsilon(\tau, \psi, dx)^{\dim \sigma} (\det \sigma)(\gamma).$$

**Démonstration.** Voir la proposition 4.13 de [14]. ■

## 2.5 Le cas archimédien

On définit ici les groupes de Weil et Weil-Deligne, les fonctions $L$ et les signes locaux dans le cas archimédien.

Il se présente deux cas distincts :

1. Le cas où $K = \mathbb{R}$
2. Le cas où $K = \mathbb{C}$

Commençons par définir les groupes de Weil et Weil-Deligne. La première chose à noter est que dans le cas archimédien, il n'y a pas de différence entre ces deux groupes : $\mathcal{WD}_K = \mathcal{W}_K$.

**Définition 2.5.1.**
1. Le cas où $K = \mathbb{R}$ : $\mathcal{W}_\mathbb{R} = \mathcal{W}(\mathbb{C}/\mathbb{R}) = \mathbb{C}^\times \cup J\mathbb{C}^\times$ où $J^2 = -1$ et $JzJ^{-1} = \bar{z}$ pour $z \in \mathbb{C}^\times$.
2. Le cas où $K = \mathbb{C}$ : $\mathcal{W}_\mathbb{C} = \mathcal{W}(\mathbb{C}/\mathbb{C}) = \mathbb{C}^\times$. On voit $\mathcal{W}_\mathbb{C}$ comme un sous-groupe d'indice 2 de $\mathcal{W}_\mathbb{R}$.

On veut désormais associer une fonction $L$ et un signe local à une représentation de $\mathcal{W}_\mathbb{R}$ (ou $\mathcal{W}_\mathbb{C}$). On commence par demander que la fonction $L(\sigma, s)$ (resp. le signe local $W(\sigma)$) pour une représentation de $\mathcal{W}_\mathbb{R}$ (ou $\mathcal{W}_\mathbb{C}$) ne dépende que de la semi-simplifié $\sigma^{ss}$ de $\sigma$ et que $L(\sigma_1 \oplus \sigma_2, s) = L(\sigma_1, s)L(\sigma_2, s)$ (resp $W(\sigma_1 \oplus \sigma_2) = W(\sigma_1)W(\sigma_2)$). Il nous suffit donc de définir $L(\sigma, s)$ (resp $W(\sigma)$) pour une représentation irréductible.

Enfin, on note de façon classique

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt,\ \Gamma_\mathbb{R}(s) = \pi^{-s/2}\Gamma(s/2) \text{ et } \Gamma_\mathbb{C}(s) = 2(2\pi)^{-s}\Gamma(s).$$

On rappelle aussi que $\Gamma_\mathbb{R}(s)\Gamma_\mathbb{R}(s+1) = \Gamma_\mathbb{C}(s)$.

**Définition 2.5.2.**
1. Le cas où $K = \mathbb{C}$ : Une représentation irréductible de $\mathcal{W}_\mathbb{C}$ est de dimension 1 et de la forme $\sigma(z) = |z|^{2s_0}(z/|z|)^m$ avec $s_0 \in \mathbb{C}$ et $m \in \mathbb{Z}$. On pose alors
$$L(\sigma, s) = \Gamma_\mathbb{C}(s + s_0 + |m|/2)$$
et
$$W(\sigma) = i^{-|m|}.$$
2. Le cas où $K = \mathbb{R}$ : Il y a dans ce cas deux types de représentations irréductibles possibles :
   (a) Soit $\sigma = \chi \circ \pi$ où $\pi$ : $\begin{array}{ccc} \mathcal{W}_\mathbb{R} & \longrightarrow & \mathbb{R}^\times \\ J & \to & -1 \\ z & \to & |z|^2 \end{array}$ et $\chi(t) = |t|^{s_0}(t/|t|)^m$ avec $s_0 \in \mathbb{C}$ et $m \in \{0, 1\}$. On pose alors
   $$L(\sigma, s) = \Gamma_\mathbb{R}(s + s_0 + m)$$
   et
   $$W(\sigma) = i^{-m}.$$
   (b) Soit $\sigma = Ind_{\mathbb{C}/\mathbb{R}}\chi$ où $\chi$ est un caractère de $\mathcal{W}_\mathbb{C}$ et $\chi(z) = |z|^{2s_0}(z/|z|)^m$ avec $s_0 \in \mathbb{C}$ et $m \in \mathbb{Z}$. On pose alors :
   $$L(\sigma, s) = \Gamma_\mathbb{C}(s + s_0 + |m|/2)$$
   et
   $$W(\sigma) = i^{-m}.$$

**Exemple 2.5.3.** Dans le cas d'une courbe elliptique $E$, on obtient :
1. Le cas où $K = \mathbb{C}$ : $L(E/\mathbb{C}, s) = \Gamma_\mathbb{C}(s)^2 = (2(2\pi)^{-s}\Gamma(s))^2$ et $W(E/\mathbb{C}) = -1$.
2. Le cas où $K = \mathbb{R}$ : $L(E/\mathbb{R}, s) = \Gamma_\mathbb{C}(s) = 2(2\pi)^{-s}\Gamma(s)$ et $W(E/\mathbb{R}) = -1$.

**Exemple 2.5.4.** Dans le cas d'une variété abélienne $A$, on a notamment : $W(A/\mathbb{C}) = W(A/\mathbb{R}) = (-1)^{\dim A}$.

# Chapitre 3

# Conjectures de parité

## 3.1 Les groupes de Selmer

### 3.1.1 Définition générale

Soit $K$ un corps de nombres et $M$ un $G_K$-module. Pour toute place $v$ de $K$, on peut voir le groupe de décomposition $G_{K_v}$ comme un sous-groupe de $G_K$ (i.e on fixe un plongement de $\bar{K}$ dans $\bar{K}_v$) et on a les applications de restrictions suivantes :

$$\mathrm{Res}_v : H^i(K, M) \longrightarrow H^i(K_v, M)$$

où on a noté $H^i(K, M)$ pour $H^i(G_K, M)$ et $H^i(K_v, M)$ pour $H^i(G_{K_v}, M)$.

**Définition 3.1.1.** Soit $v \nmid \infty$, $K_v$ le complété de $K$ en $v$ et $K_v^{nr}$ son extension maximale non-ramifié. On appellera groupe de cohomologie non-ramifié le sous-groupe $H^1_{nr}(K_v, M)$ de $H^1(K_v, M)$ défini par :

$$H^1_{nr}(K_v, M) = \ker\left[H^1(K_v, M) \xrightarrow{\mathrm{Res}} H^1(K_v^{nr}, M)\right].$$

**Définition 3.1.2.** Une structure de Selmer $\mathcal{F}$ pour $A$ est une collection de sous-groupes

$$H^1_{\mathcal{F}}(K_v, M) \subset H^1(K_v, M)$$

pour toute place $v$ de $K$, tel que $H^1_{\mathcal{F}}(K_v, M) = H^1_{nr}(K_v, M)$ pour presque tout $v$.

**Définition 3.1.3.** Si $\mathcal{F}$ est une structure de Selmer pour $M$ alors on définit le groupe de Selmer $H^1_{\mathcal{F}}(K, M)$ par :

$$H^1_{\mathcal{F}}(K, M) = \ker\left[H^1(K, M) \xrightarrow{\prod \mathrm{Res}_v} \prod_v \left(H^1(K_v, M)/H^1_{\mathcal{F}}(K_v, M)\right)\right].$$

Autrement dit, $H^1_{\mathcal{F}}(K, M)$ est le sous-groupe des classes de $H^1(K, M)$ dont la localisation appartient à $H^1_{\mathcal{F}}(K_v, M)$ pour tout $v$.

**Exemple 3.1.4.** Soit $K$ un corps de nombres, $A/K$ une variété abélienne et $m > 0$. On a pour tout $v$ la suite exacte suivante :

$$0 \longrightarrow A(K_v)/mA(K_v) \longrightarrow H^1(K, A[m]) \longrightarrow H^1(K, A(\bar{K}_v))[m] \longrightarrow 0.$$

On pose alors, pour toute place $v$, $H^1_{\mathcal{F}}(K_v, A[m]) = \mathrm{Im}\left[A(K_v)/mA(K_v) \hookrightarrow H^i(K, A[m])\right]$. Si $v \nmid m\infty$ et $A$ a bonne réduction en $v$ alors $H^1_{\mathcal{F}}(K, A[m]) = H^1_{nr}(K_v, A[m])$ et par conséquent la collection de sous-groupes $\{H^1_{\mathcal{F}}(K_v, A[m])\}$ est une structure de Selmer et le groupe $H^1_{\mathcal{F}}(K, A[m])$ est le classique groupe de Selmer $S(A/K, m)$ (voir par exemple [59] p.297).

### 3.1.2 Le cas d'une représentation $\mathfrak{p}$-adique

Soit $K$ et $E$ deux corps de nombres et $\sigma : G_K \longrightarrow GL(V_\mathfrak{p}) \simeq GL_n(E_\mathfrak{p})$ une représentation $\mathfrak{p}$-adique de $G_K$ (où $\mathfrak{p} \mid p$ et donc $[E_\mathfrak{p} : \mathbb{Q}_p] < \infty$). Le $E_\mathfrak{p}[G]$-module $V_\mathfrak{p}$ admet un $\mathcal{O}_{E_\mathfrak{p}}$-réseau stable $T_\mathfrak{p}$ par $G_K$ (on notera $T$ et $V$ pour $T_\mathfrak{p}$ et $V_\mathfrak{p}$). On pose de plus $W = V/T$ et $W_M = M^{-1}T/T$ (pour $M \in \mathcal{O}_{E_\mathfrak{p}}$), autrement dit $W_M$ est la $M$-torsion de $W$ et $\varprojlim W_M = T$.

**Définition 3.1.5.** Pour toute place $v$ de $K$, on définit les sous-groupes

$$H^1_f(K_v, T), H^1_f(K_v, V), H^1_f(K_v, W) \text{ et } H^1_f(K_v, W_M)$$

de

$$H^1(K_v, T), H^1(K_v, V), H^1(K_v, W) \text{ et } H^1(K_v, W_M) \text{ respectivement}$$

de la façon suivante :

1. Si $v \nmid p\infty$ alors on pose $H^1_f(K_v, V) = H^1_{nr}(K_v, V)$ puis

   $$H^1_f(K_v, T) = \alpha^{-1}(H^1_f(K_v, V)), H^1_f(K_v, W) = \beta(H^1_f(K_v, V))$$

   et

   $$H^1_f(K_v, W_M) = \gamma^{-1}(H^1_f(K_v, W))$$

   où les applications $\alpha$, $\beta$ et $\gamma$ sont les applications naturelles suivantes

   $$H^1(K_v, T) \xrightarrow{\alpha} H^1(K_v, V) \xrightarrow{\beta} H^1(K_v, W)$$

   et

   $$H^1(K_v, W_M) \xrightarrow{\gamma} H^1(K_v, W).$$

2. Si $v \mid p$ alors on pose $H^1_f(K_v, V) = \ker\left[H^1(K_v, V) \longrightarrow H^1(K_v, V \otimes B_{cris})\right]$, où $B_{cris}$ est l'anneau défini par Fontaine (voir par exemple [6] §3).
3. Si $v \mid \infty$ alors $H^1(K_v, V) = 0$ donc $H^1_f(K_v, V) = 0$ puis (en procédant comme en 1.) $H^1_f(K_v, T) = H^1(K_v, T)$ et $H^1_f(K_v, W) = 0$.

**Proposition 3.1.6.** Soit $T$ comme ci-dessus et $v \nmid p\infty$ alors :

1. $H^1_f(K_v, W) = H^1(K_v, W)_{\text{div}}$.
2. $H^1_{nr}(K_v, T) \subset H^1_f(K_v, T)$ est d'indice fini et $H^1(K_v, T)/H^1_f(K_v, T)$ est sans torsion.
3. Si $T$ est non-ramifié alors $H^1_f(K_v, T) = H^1_{nr}(K_v, T)$ et $H^1_f(K_v, W) = H^1_{nr}(K_v, W)$.

**Démonstration.** Voir lemme 1.3.5 de [50]. ■

**Proposition 3.1.7.** On a les suites exactes et isomorphismes verticaux suivants :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1_f(K_v, W) & \longrightarrow & H^1(K_v, W) & \longrightarrow & H^1_s(K_v, W) & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & \varinjlim H^1_f(K_v, W_M) & \longrightarrow & \varinjlim H^1(K_v, W_M) & \longrightarrow & \varinjlim H^1_s(K_v, W_M) & \longrightarrow & 0
\end{array}$$

et

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1_f(K_v, T) & \longrightarrow & H^1(K_v, T) & \longrightarrow & H^1_s(K_v, T) & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & \varprojlim H^1_f(K_v, W_M) & \longrightarrow & \varprojlim H^1(K_v, W_M) & \longrightarrow & \varprojlim H^1_s(K_v, W_M) & \longrightarrow & 0
\end{array}$$

où on a noté $H^1_s(K_v, \cdot)$ pour $H^1(K_v, \cdot)/H^1_f(K_v, \cdot)$.

**Démonstration.** Voir Corollaire 1.3.10 de [50]. ■

**Définition-Proposition 3.1.8.** Soit $\sigma : G_K \longrightarrow GL(V) \simeq GL_n(E_{\mathfrak{p}})$ une représentation $\mathfrak{p}$-adique de $G_K$, non-ramifiée en $v$ pour presque toute place $v$ de $K$ alors la collection de sous-groupes $\left\{H^1_f(K_v, V/T)\right\}$ est une structure de Selmer et on pose :

$$H^1_f(K, V/T) = \ker\left[H^1(K, V/T) \overset{\prod \mathrm{Res}_v}{\longrightarrow} \prod_v \left(H^1(K_v, V/T)/H^1_f(K_v, V/T)\right)\right].$$

### 3.1.3 Le cas des variétés abéliennes

Soit $K$ un corps de nombres, $A/K$ une variété abélienne et $T := T_p(A)$ le module de Tate alors on a une représentation $\sigma_A : G_K \longrightarrow GL(V)$ (où $V := V_p(A)$), $W = V/T = A[p^\infty]$ et $W_{p^n} = A[p^n]$. On obtient $H^1(K_v, A[p^\infty]) = \varinjlim H^1(K_v, A[p^n])$ et $H^1_f(K_v, A[p^\infty]) = \varinjlim H^1_f(K_v, A[p^n])$ et $S(A/K, p^\infty) := H^1_f(K, V/T) = \varinjlim S(A/K, p^n)$. Le $p^\infty$-groupe de Selmer $S(A, p^\infty)$ vérifie la suite exacte suivante :

$$0 \longrightarrow A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow S(A/K, p^\infty) \longrightarrow Ш(A, p^\infty) \longrightarrow 0$$

où $Ш(A, p^\infty)$ est défini ci-dessous.

**Définition 3.1.9.** On appelle dual du $p^\infty$-groupe de Selmer $S(A, p^\infty)$ et on note $S_p(A/K)$ le groupe suivant :

$$S_p(A/K) := Hom_{\mathbb{Z}_p}(S(A/K, p^\infty), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

**Définition 3.1.10.** On appelle groupe de Tate-Shafarevitch et on note $Ш(A/K)$ le groupe

$$Ш(A/K) = \ker\left(H^1(Gal(\bar{K}/K), A) \to \prod_v H^1(Gal(\bar{K}_v/K_v), A)\right).$$

De plus, on note $Ш(A, p^n)$ sa $p^n$-torsion. Ainsi $Ш(A, p^n) = Ш(A/K)[p^n]$ et $Ш(A, p^\infty) = Ш(A/K)[p^\infty]$.

**Proposition 3.1.11.** Si on pose $rg_p(A/K) := \dim_{\mathbb{Q}_p} S_p(A/K)$ alors :

$$rg_p(A/K) = rg(A/K) + a$$

où $a$ est le nombre de copies de $\mathbb{Q}_p/\mathbb{Z}_p$ dans le groupe de Tate-Shafarevitch et $rg(A/K)$ est le rang du groupe de Mordell-Weil de $A$ sur $K$.

**Démonstration.** En appliquant $Hom_{\mathbb{Z}_p}(\cdot, \mathbb{Q}_p/\mathbb{Z}_p)$ ($\mathbb{Q}_p/\mathbb{Z}_p$ est un $\mathbb{Z}_p$-module injectif) à la suite exacte

$$0 \longrightarrow A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow S(A/K, p^\infty) \longrightarrow Ш(A/K, p^\infty) \longrightarrow 0$$

puis en tensorisant par $\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ ($\mathbb{Q}_p$ est plat sur $\mathbb{Z}_p$) on obtient :

$$0 \longrightarrow Ш_p(A/K) \longrightarrow S_p(A/K) \longrightarrow Hom_{\mathbb{Z}_p}(A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow 0$$

où $Ш_p(A/K) = Hom_{\mathbb{Z}_p}(Ш(A, p^\infty), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Comme $S(A/K, p^\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{rg_p(A/K)} \oplus$ (partie finie), $A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{rg(A/K)}$ et $Ш(A/K, p^\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^a \oplus$(partie finie), la suite exacte ci-dessus fournit le résulat. ■

Ainsi toute la différence entre $rg_p(A/K)$ et $rg(A/K)$ est "contenue" dans le groupe de Tate-Shafarevitch. La difficile conjecture suivante entraîne notamment que $rg_p(E/K) = rg(E/K)$ pour tout $p$.

**Conjecture 3.1.12.** Le groupe de Tate-Shafarevitch $Ш(A/K)$ est fini.

## 3.2 Les conjectures

### 3.2.1 Le cas des prémotifs.

Soit $M = \{\sigma_{\mathfrak{p}}\}$ un prémotif sur $K$ et $\iota$ un plongement de $E$ dans $\mathbb{C}$. Dans toutes les définitions et conjectures ci-dessous, il est possible de remplacer prémotif par famille faiblement compatible (on a vu qu'on conjecture que ces deux notions sont identiques) On a vu que pour toute place $v$ de $K$, on peut définir une représentation $\sigma_{\iota M,v}$ de $\mathcal{WD}_K$ (à partir de n'importe quel $\sigma_{\mathfrak{p}}$ tel que $l_v \neq l_{\mathfrak{p}}$ et $\iota_{\mathfrak{p}}$ plongement de $E_{\mathfrak{p}}$ dans $\mathbb{C}$ qui prolonge $\iota$) qui est indépendante des choix de $\mathfrak{p}$ et $\iota_{\mathfrak{p}}$. On complète la fonction $L(\iota M, s) = \prod_{v \text{ finie}} L(\sigma_{\iota M,v}, s)$ en une fonction $L$ "complète" $\Lambda(\iota M, s) = \prod_v L(\sigma_{\iota M,v}, s)$ (Les fonctions $L(\sigma_{\iota M,v}, s)$ ont été définies en 2.2 et 2.5 pour les places finies et les places archimédiennes respectivement).

**Définition 3.2.1.** On dit que le prémotif $M$ est de poids $w$, si pour $\alpha \in \mathbb{C}^\times$ tel que $B_{\mathfrak{q}}(\alpha^{-1}) = 0$ et pour tout $\tau \in Aut(\mathbb{C})$, on a :

$$|\tau(\alpha)| = (N\mathfrak{q})^{w/2} \text{ si } \mathfrak{q} \notin S$$

où $S$ est l'ensemble des places qui apparait dans la définition d'une famille compatible de représentation.

**Remarque 3.2.2.**
1. On définit de la même façon le poids d'une classe d'isomorphisme de représentations complètement (ou faiblement) compatibles.
2. Cette définition permet de dire que la fonction $L(\iota M, s)$ (et donc $\Lambda(\iota M, s)$) est convergente pour $\operatorname{Re} s > w/2 + 1$.
3. Le fait que ce soit "pour tout $\tau \in Aut(\mathbb{C})$" permet que la définition du poids ne dépende pas du choix du plongement de $E$ dans $\mathbb{C}$.

**Définition 3.2.3.** Une représentation $\sigma$ de $\mathcal{W}_K$ est dite essentiellement auto-duale de poids $w$ si :

$$\sigma \simeq \sigma^* \otimes \omega^{-w}.$$

**Définition 3.2.4.** On dit que le prémotif $M$ est essentiellement auto-dual de poids $w$ si :

$$\text{pour toutes places } v \text{ de } K,\ \sigma_{\iota M,v} \simeq \sigma^*_{\iota M,v} \otimes \omega^{-w}.$$

**Remarque 3.2.5.** Un prémotif essentiellement auto-dual de poids $w$ est un prémotif de poids $w$.

On a alors la conjecture suivante :

**Conjecture 3.2.6.**
1. La fonction $\Lambda(\iota M, s)$ se prolonge en une fonction holomorphe sur $\mathbb{C}$.
2. Soit $W(\iota M) = \prod_v W(\sigma_{\iota M,v})$ (c'est une constante de module 1), la fonction $\Lambda(\iota M, s)$ vérifie l'équation fonctionnelle :

   $$\Lambda(\iota M, s) = W(\iota M)\Lambda(\iota M^*, k - s)$$

   où $k = w + 1$.
   Dans le cas d'un prémotif essentiellement auto-dual de poids impair $w$, on obtient :

   $$\Lambda(\iota M, s) = W(\iota M)\Lambda(\iota M, w + 1 - s)$$

   où $W(\iota M) \in \{\pm 1\}$.

**Conjecture 3.2.7** (Bloch-Kato)**.** Soit $M = \{\sigma_{\mathfrak{p}} : G_K \longrightarrow GL(V_{\mathfrak{p}})\}$ un prémotif essentiellement auto-dual de poids impair $w$ sur $K$ et $T_{\mathfrak{p}}$ un $\mathcal{O}_{E_{\mathfrak{p}}}$-réseau $G_K$-stable de $V_{\mathfrak{p}}$ alors si on pose $S_{\mathfrak{p}}(M/K) := Hom_{\mathcal{O}_{E_{\mathfrak{p}}}}(H^1_f(K, M_{\mathfrak{p}}), E_{\mathfrak{p}}/\mathcal{O}_{E_{\mathfrak{p}}}) \otimes_{\mathcal{O}_{E_{\mathfrak{p}}}} E_{\mathfrak{p}}$ (où $H^1_f(K, M_{\mathfrak{p}}) := H^1_f(K, V_{\mathfrak{p}}/T_{\mathfrak{p}})$ voir définition-proposition 3.1.8) et $rg_{\mathfrak{p}}M := \dim_{E_{\mathfrak{p}}} S_{\mathfrak{p}}(M/K)$ on a :

$$rg_{\mathfrak{p}}M = ord_{s=\frac{w+1}{2}}\Lambda(\iota M, s).$$

**Remarque 3.2.8.**
1. Dans ce cas, les facteurs $\Gamma$ n'ont pas de pôle en $s = \frac{w+1}{2}$ et donc $ord_{s=\frac{w+1}{2}}\Lambda(\iota M, s) = ord_{s=\frac{w+1}{2}}L(\iota M, s)$.
2. La conjecture implique en particulier que l'ordre d'annulation de $\Lambda(\iota M, s)$ en $s = \frac{w+1}{2}$ ne dépend pas de $\iota$ (si $M$ provient d'un motif, c'est la conjecture de Deligne-Gross, voir Conjecture 2.7 (ii) p.323 de [13]).

**Conjecture 3.2.9.** Soit $M = \{\sigma_{\mathfrak{p}}\}$ un prémotif essentiellement auto-dual de poids impair $w$ sur $K$ alors :

$$(-1)^{rg_{\mathfrak{p}}M} = W(\iota M).$$

**Remarque 3.2.10.** Rohrlich a montré que $W(\iota M)$ est indépendant de $\iota$ (sous réserve d'une condition sur le déterminant des $\sigma_{\iota M,v}$ qui est satisfaite si $M$ est essentiellement symplectique) dans [47].

Soit $L/K$ une extension finie et $\tau$ une $E$-représentation auto-duale d du groupe de Galois $G_{L/K} := Gal(L/K)$, $M \otimes \tau = \left\{\sigma_{\mathfrak{p}} \otimes \tau : G_K \longrightarrow GL(V'_{\mathfrak{p}})\right\}$ et $T'_{\mathfrak{p}}$ un $\mathcal{O}_{E_{\mathfrak{p}}}$-réseau $G_K$-stable de $V'_{\mathfrak{p}}$ alors si on note $H^1_f(K, M_{\mathfrak{p}} \otimes \tau) := H^1_f(K, V'_{\mathfrak{p}}/T'_{\mathfrak{p}})$ on a :

$$\begin{aligned} H^1_f(K, M_{\mathfrak{p}} \otimes \tau) &= H^1_f(L, M_{\mathfrak{p}} \otimes_E \tau)^{G_{L/K}} \\ &= (H^1_f(L, M_{\mathfrak{p}}) \otimes_E \tau)^{G_{L/K}} \\ &= Hom_{E[G_{L/K}]}(\tau^*, H^1_f(L, M_{\mathfrak{p}})) \\ &= Hom_{E[G_{L/K}]}(\tau, H^1_f(L, M_{\mathfrak{p}})). \end{aligned}$$

En notant par ailleurs $\Lambda(M, \tau, s) = \prod_v L(\sigma_{M,v} \otimes \tau, s)$ et $W(M, \tau) = \prod_v W(\sigma_{M,v} \otimes \tau)$, on obtient la conjecture suivante :

**Conjecture 3.2.11.** Soit $M = \{\sigma_{\mathfrak{p}}\}$ un prémotif essentiellement auto-dual de poids impair $w$ sur $K$ et $\tau$ est une représentation auto-duale de $G(L/K)$ alors :

$$\Lambda(M, \tau, s) = W(M, \tau)\Lambda(M, \tau, w + 1 - s).$$

De plus, si $m_\tau$ désigne la multiplicité de $\tau$ dans $H^1_f(L, M_{\mathfrak{p}})$ alors (Bloch-Kato avec twist) :

$$m_\tau = ord_{s=\frac{w+1}{2}}\Lambda(M/K, \tau, s)$$

et (conjecture de $p$-parité avec twist),

$$(-1)^{m_\tau} = W(M/K, \tau).$$

### 3.2.2 Le cas des variétés abéliennes

Si $A/K$ est une variété abélienne alors la famille $\{\sigma_p\}_p$ (où $\sigma_p : G_K \longrightarrow GL(V_p(A))$) forment une famille de représentations $p$-adique complètement compatible qui est prémotivique (voir la remarque 1.4.7). On réénonce les conjectures précédentes dans le cas des variétés abéliennes :

**Conjecture 3.2.12** (Prolongement holomorphe et équation fonctionnelle)**.** Si $A/K$ est une variété abélienne, alors $\Lambda(A/K, s)$ qui converge pour $\mathrm{Re}\, s > \frac{3}{2}$ admet un prolongement holomorphe sur $\mathbb{C}$ et vérifie l'équation fonctionnelle suivante :

$$\Lambda(A/K, s) = W(A/K)\Lambda(A/K, 2-s)$$

où $\Lambda(A/K, s) = \Gamma_{\mathbb{C}}(s)^{[K:\mathbb{Q}]\dim A} L(A/K, s)$.

**Remarque 3.2.13.** La conjecture est connue (avec un prolongement méromorphe, pas holomorphe) pour une variété abélienne de type $GL(2)$ définie sur $F \subset K$ totalement réel ou à multiplication complexe pour lequel $Gal(K/F)$ est abélien ou diédral. Voir [63] (pour $F = \mathbb{Q}$) et [2].

**Conjecture 3.2.14** (BSD pour les groupes de Selmer)**.** Si $A/K$ est une variété abélienne et si on pose $X_p(A/K) := Hom_{\mathbb{Z}_p}(S(A/K, p^\infty), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ et $rg_p(A/K) := \dim_{\mathbb{Q}_p} X_p(A/K)$ alors

$$rg_p(A/K) = ord_{s=1}\Lambda(A/K, s).$$

En particulier, la combinaison de la conjecture sur la finitude de $Ш(A/K)$ (dans ce cas $rg_p(A/K) = rg(A/K)$) et la conjecture précédente donne la classique conjecture de Birch et Swinnerton-Dyer :

**Conjecture 3.2.15** (BSD)**.** Si $A/K$ est une variété abélienne alors

$$rg(A/K) = ord_{s=1}\Lambda(A/K, s).$$

**Remarque 3.2.16.** Le facteur $\Gamma_{\mathbb{C}}(s)$ n'ayant pas de pôle en 1, dans les deux conjectures ci-dessus $ord_{s=1}\Lambda(A/K, s) = ord_{s=1}L(A/K, s)$.

Et enfin en combinant ces conjectures, on obtient les conjectures plus faibles suivantes :

**Conjecture 3.2.17** (de parité)**.** Si $A/K$ est une variété abélienne alors :

$$(-1)^{rg(A/K)} = W(A/K).$$

**Remarque 3.2.18.** Dans [18], les frères Dokchitser ont montré que cette conjecture est vraie dans le cas où $A$ est une courbe elliptique conditionnellement à la finitude des parties $2^\infty$ et $3^\infty$ torsion du groupe de Tate-Shafarevitch de $A/K(A[2])$.

**Conjecture 3.2.19** (de $p$-parité)**.** Si $A/K$ est une variété abélienne alors :

$$(-1)^{rg_p(A/K)} = W(A/K).$$

**Remarque 3.2.20.**

1. Les frères Dokchitser ont démontré dans [20] que pour $A$ une courbe elliptique sur $\mathbb{Q}$ la conjecture est vraie pour tout nombre premier $p$.
2. Si $A$ est une courbe elliptique, et $L/K$ une extension galoisienne de degré impair alors la conjecture de $p$-parité est vraie pour $A/L$ si et seulement si elle est vraie pour $A/K$. Ce résultat qui repose essentiellement sur l'auto-dualité du groupe de Selmer $S_p(E/L)$ en tant que $\mathbb{Q}_p[G]$-représentation (due initialement à Jan Nekovář dans un contexte très général dans [37] et redémontré dans le cas des courbes elliptiques par Tim et Vladimir Dokchitser dans [19]).
3. Les deux points précédents donnent notamment que : Si $K$ est une extension galoisienne de degré impair de $\mathbb{Q}$ et $A/K$ est une courbe elliptique alors la conjecture de $p$-parité est vraie pour $A/K$.

4. De la même façon, on peut montrer (voir [19]) que : Si $A$ est une courbe elliptique et $L/K$ une extension abélienne, la conjecture de $p$-parité est vraie pour $A/L$ si et seulement si elle est vraie pour $A/K$. On peut donc en déduire que : Si $K$ est une extension abélienne de $\mathbb{Q}$ et $A/K$ est une courbe elliptique alors la conjecture de $p$-parité est vraie pour $A/K$.
5. Dans le même ordre d'idées, dans [21] ils obtiennent notamment que pour $A/\mathbb{Q}$ une courbe elliptique, $p > 2$, $m, n \geqslant 1$ entiers et $K \subset \mathbb{Q}(\mu_{p^n}, \sqrt[n]{m})$ la conjecture est vérifiée.

**Conjecture 3.2.21** (de $p$-parité avec twist)**.** Soit $L/K$ une extension finie de corps de nombres, $A/K$ une variété abélienne et $\tau$ une $\mathbb{C}$-représentation auto-duale de $G(L/K)$ alors :

$$(-1)^{\langle \tau, S_p(A/L)\rangle} = W(A/K, \tau)$$

où $\langle \tau, \cdot \rangle$ désigne le classique produit scalaire de $\tau$ avec le complexifié de $\cdot$.

**Remarque 3.2.22.**
1. Tim et Vladimir Dokchitser ont démontré dans [21] ce résultat dans le cas où $A$ est une courbe elliptique, $p \equiv 3 \bmod 4$, $K = \mathbb{Q}$, $L$ est une $p$-extension d'une extension abélienne de $K$ et $\tau$ une représentation orthogonale.
2. Les résultats du chapitre 4 nous permettront notamment d'améliorer ce résultat en remplaçant la condition "$p \equiv 3 \bmod 4$" par "$p \geq 3$".

## 3.3 Signes locaux des courbes elliptiques

Soit $K$ une extension finie de $\mathbb{Q}_l$.
Les résultats de cette section sont dus à Rohrlich et exposés dans [46].
On considère les représentations $\sigma$ de $\mathcal{W}_K$ vérifiant :
· $\sigma$ est irréductible.
· $\sigma$ est symplectique.
· $\sigma = Ind_{H/K}\varphi$ où $H$ est une extension quadratique non-ramifiée de $K$ et $\varphi$ est un caractère modérement ramifié de $H^\times$. En particulier $\dim \sigma = 2$.

Ce sont précisément, les représentations de $\mathcal{W}_K$ qui sont de dimension 2, irréductibles, symplectiques et modérément ramifiées comme nous le verrons (comme cas particulier de la description des représentations irréductibles, symplectiques et modérément ramifiées de $\mathcal{W}_K$) au chapitre 5.

**Théorème 3.3.1.** Soit $\tau$ une représentation auto-duale de $G_K$ alors :

$$W(\sigma \otimes \tau) = (\det \tau)(-1)\varphi(u_{H/K})^{\dim \tau}(-1)^{\langle 1+\eta+\hat{\sigma}, \tau\rangle},$$

où $u_{H/K} \in \mathcal{O}_K^\times$ tel que $H = K(u_{H/K})$ et $u_{H/K}^2 \in K$, $\eta = \chi_{H/K}$ le caractère quadratique de $K^\times$ correspondant à $H$, $\hat{\sigma} = ind_{H/K}\hat{\varphi}$ avec $\hat{\varphi} = \theta\varphi$ et $\theta$ le caractère non-ramifié de $H^\times$.

**Démonstration.** C'est le théorème 1 p.318 de [46]. ■

Dans le cadre des courbes elliptiques, ce théorème permet d'obtenir :

**Théorème 3.3.2.** Soit $E$ une courbe elliptique sur $K$ et $\tau$ une représentation auto-duale de $G_K$ alors :

1. Si $E$ a réduction potentiellement multiplicative alors :
$$W(\sigma'_{E/K} \otimes \tau) = (\det \tau)(-1)\chi(-1)^{\dim \tau}(-1)^{\langle \chi, \tau \rangle}$$
où $\chi$ est le caractère de $K^\times$ associé à l'extension $K(\sqrt{c_6})$ de $K$ (i.e la corps où $E$ acquière réduction multiplicative déployée).
2. Si $E$ a potentiellement bonne réduction alors $\sigma'_{E/K} = \sigma_{E/K}$ et si $l \geq 5$ on a :
$$W(\sigma'_{E/K} \otimes \tau) = \begin{cases} (\det \tau)(-1)(-W(E/K))^{\dim \tau}(-1)^{\langle 1+\eta+\hat{\sigma}, \tau \rangle} & \text{si } \sigma_{E/K} \text{ est irréd,} \\ (\det \tau)(-1)(W(E/K))^{\dim \tau} & \text{sinon.} \end{cases}$$

**Démonstration.** C'est le théorème 2 p.329 de [46]. ∎

**Remarque 3.3.3.** Le résultat de Rohrlich est même plus précis. Il donne précisément la valeur de $W(E/K)$. En effet, si $e = \frac{12}{\text{pgcd}(v(\Delta),12)}$ alors
$$W(E/K) = \begin{cases} 1 & \text{si } f(K/\mathbb{Q}_p) \text{ est paire ou } e = 1, \\ \left(\frac{-1}{p}\right) & \text{si } f(K/\mathbb{Q}_p) \text{ est impaire et } e = 2 \text{ ou } 6, \\ \left(\frac{-3}{p}\right) & \text{si } f(K/\mathbb{Q}_p) \text{ est impaire et } e = 3, \\ \left(\frac{-2}{p}\right) & \text{si } f(K/\mathbb{Q}_p) \text{ est impaire et } e = 4. \end{cases}$$

De plus, il montre que si $q$ est le cardinal du corps résiduel $k_K$ de $K$ (donc une puissance de $l$) alors $\sigma_{E/K}$ est irréductible si et seulement si $q \equiv -1 \bmod e$.

**Remarque 3.3.4.** Nous généraliserons le résultat du théorème 3.3.1 et le 2. du théorème 3.3.2 au chapitre 5.

## 3.4 Les constantes de régulation et la conjecture de parité

Cette section reprend les résultats des frères Dokichitser dans l'article "Regulator constants and the parity conjecture" (voir [18]).

### 3.4.1 Les relations entre les représentations de permutations

Soit $G$ un groupe fini et $S$ l'ensemble de ses sous-groupes à conjugaison près.

**Définition 3.4.1.** On appellera anneau de Burnside le groupe abélien libre $\mathbb{Z}S$ (on n'utilisera pas la structure multiplcative de l'anneau). On notera $\sum_i n_i H_i$ un élément de $\mathbb{Z}S$ (où on note encore $H_i$ la classe de $H_i$ modulo la conjugaison). On notera par ailleurs $H^x = xHx^{-1}$.

**Définition 3.4.2.** On appellera $G$-relation un élément $\Theta = \sum_i n_i H_i$ de l'anneau de Burnside de $G$ tel que $\bigoplus_i \mathbb{C}[G/H_i]^{n_i} \simeq 0$, où $\mathbb{C}[G/H] \simeq Ind_H^G 1_H$. Autrement dit, le caractère $\sum_i n_i \chi_{\mathbb{C}[G/H_i]}$ est nul.

**Exemple 3.4.3.**
1. Un groupe cyclique n'a pas de relations non-triviales.
2. $G = C_2 \times C_2$ a 5 sous-groupes $\{1\}$, $C_2^a = C_2 \times \{1\}$, $C_2^b = \{1\} \times C_2$, $C_2^c = \{(1,1), (-1,-1)\}$ et $G$. On a alors une unique $G$-relation (à un multiple près) :
$$\Theta = \{1\} - C_2^a - C_2^b - C_2^c + 2G.$$

3. Si $G = D_{2n} = C_n \rtimes C_2$ avec $n$ impair alors :

$$\Theta = \{1\} - 2C_2 - C_n + 2G$$

est une $G$-relation.

**Théorème 3.4.4.** Soit $G$ un groupe, $D, H_i$ des sous groupes de $G$ et $N$ un sous-groupe distingué de $G$. On a les propriétés suivantes :

1. La somme et la différence de deux $G$-relations est une $G$-relation.
2. Si $\Theta = \sum_i n_i H_i$ et $m\Theta$ est une $G$-relations alors $\Theta$ est une $G$-relation.
3. (Relèvement) Si $H_i \supset N$ et $\sum_i n_i H_i/N$ est une $G/N$-relation alors $\sum_i n_i H_i$ est une $G$-relation.
4. (Induction) Si $\Theta = \sum_i n_i H_i$ est une $D$-relation alors $Ind_D^G \Theta = \sum_i n_i H_i$ est une $G$-relation.
5. (Projection) Si $\sum_i n_i H_i$ est une $G$-relation alors $\mathrm{Proj}_{G/N} \Theta = \sum_i n_i (H_i N)/N$ est une $G/N$-relation.
6. (Restriction) Si $\Theta = \sum_i n_i H_i$ est une $G$-relation alors :

$$\operatorname*{Res}_D \Theta = \sum_i n_i \sum_{x \in H_i \backslash G / D} D \cap H_i^{x^{-1}} \text{est une } D\text{-relation.}$$

**Démonstration.** Voir le Théorème 2.8 de [18]. ■

**Remarque 3.4.5.** Pour une étude détailler des $G$-relations en fonction du groupe $G$, on pourra consulter les articles [3] et [4].

### 3.4.2 Les constantes de régulation.

On considère un corps $K$ de caractéristique 0.

**Définition 3.4.6.** Soit $G$ un groupe fini, $\rho$ une $K[G]$-représentation auto-duale et $\Theta = \sum_i n_i H_i$ une $G$-relation. On choisit un accouplement $K$-bilinéaire non-dégénéré et $G$-invariant $\langle , \rangle$ sur $\rho$ à valeurs dans $L/K$ et on pose :

$$C_\Theta(\rho) = \prod_i \det\left(\frac{1}{|H_i|} \langle , \rangle \left| \rho^{H_i} \right.\right)^{n_i} \in K^\times / K^{\times 2},$$

où $\det(\langle , \rangle | V) := \det(\langle e_i, e_j \rangle_{i,j})$ pour toute base de $V$ sur $K$.

**Remarque 3.4.7.**

1. Si $\langle , \rangle_1$ et $\langle , \rangle_2$ sont deux accouplements $K$-bilinéaires, non-dégénérés et $G$-invariant à valeurs dans $L \supset K$, alors si on fixe des bases pour chaque $\rho^{H_i}$, on a :
$$\prod_i \det\left(\frac{1}{|H_i|} \langle , \rangle_1 \left| \rho^{H_i} \right.\right)^{n_i} = \prod_i \det\left(\frac{1}{|H_i|} \langle , \rangle_2 \left| \rho^{H_i} \right.\right)^{n_i} \in L^\times.$$
2. On peut choisir $\langle , \rangle_1$ à valeurs dans $K$ et donc les éléments ci-dessus sont dans $K^\times$.
3. Un changement de base de chaque $\rho^{H_i}$, revient à multiplier $\prod_i \det\left(\frac{1}{|H_i|} \langle , \rangle_1 \left| \rho^{H_i} \right.\right)^{n_i}$ par un élément de $K^{\times 2}$.

4. Les points 1 à 3 nous permettent de dire que la constante de régulation $C_\Theta(\rho)$ est bien définie, non nulle et indépendante du choix de $\langle , \rangle$.

**Lemme 3.4.8.** Soit $\Theta = \sum_i n_i H_i$ est une $G$-relation et $\rho$ une $K[G]$-représentation alors :

$$\sum_i n_i \dim \rho^{H_i} = 0.$$

**Démonstration.** On a $\sum_i n_i \dim \rho^{H_i} = \sum_i n_i \langle \mathrm{Res}_{H_i} \rho, 1_{H_i} \rangle_{H_i}$. De plus, d'après la réciprocité de Frobenius et la définition d'une $G$-relation on a :

$$\sum_i n_i \left\langle \operatorname*{Res}_{H_i} \rho, 1_{H_i} \right\rangle_{H_i} = \sum_i n_i \left\langle \rho, Ind_{H_i}^G 1_{H_i} \right\rangle_G = \left\langle \rho, \bigoplus_i \left( Ind_{H_i}^G 1_{H_i} \right)^{\oplus n_i} \right\rangle_G = 0$$

ce qui donne le résultat. ■

**Proposition 3.4.9.** Soit $G$ un groupe fini. Soient $\Theta$, $\Theta_1$ et $\Theta_2$ des $G$-relations et $\rho, \rho_1, \rho_2$ des $K[G]$-représentations auto-duales alors :

$$\begin{aligned} & C_{\Theta_1+\Theta_2}(\rho) = C_{\Theta_1}(\rho) C_{\Theta_2}(\rho) \\ \text{et} \quad & C_\Theta(\rho_1 + \rho_2) = C_\Theta(\rho_1) C_\Theta(\rho_2) \end{aligned}$$

**Démonstration.** Voir le corollaire 2.18 de [18]. ■

**Théorème 3.4.10.** Soit $\rho$ une $K[G]$-représentation auto-duale telle que $\rho \otimes_K \bar{K}$ admet un accouplement bilinéaire $G$-invariant et alterné alors :

$$C_\Theta(\rho) = 1 \text{ pour toutes } G\text{-relations } \Theta.$$

**Démonstration.** Voir le théorème 2.24 de [18]. ■

**Corollaire 3.4.11.** Soit $\rho$ une $K[G]$-représentation auto-duale si elle vérifie l'un des critères suivants :

1. La représentation $\rho \otimes_K \bar{K}$ est symplectique comme $\bar{K}[G]$-représentation.
2. La représentation $\rho \otimes_K \bar{K} \simeq \tau \oplus \tau^*$ pour une $\bar{K}[G]$-représentation $\tau$.
3. Aucune des composantes irréductibles sur $\bar{K}$ de $\rho \otimes_K \bar{K}$ n'est auto-duale.

Alors

$$C_\Theta(\rho) = 1 \text{ pour toutes } G\text{-relations } \Theta.$$

**Démonstration.** Voir Corollaire 2.25 de [18]. ■

**Lemme 3.4.12.** Soit $\rho$ une $K[G]$-représentation auto-duale et $\Theta = \sum_i n_i H_i$ une $G$-relation. Si aucune des composantes irréductibles de $\rho \otimes_K \bar{K}$ n'est une des composantes irréductibles d'un $\bar{K}[G/H_i]$ alors $C_\Theta(\rho) = 1$.

**Démonstration.** Voir le lemme 2.26 de [18]. ■

**Définition 3.4.13.** Soit $R$ un anneau principal et $K$ son corps des fractions (tel que la caractéristique de $K$ soit première avec $|G|$) et $\rho$ un $R[G]$-module auto-dual alors on peut définir comme précédemment $C_\Theta(\rho)$ par :

$$C_\Theta(\rho) = \prod_i \det \left( \frac{1}{|H_i|} \langle , \rangle \Big|_{\rho^{H_i}} \right)^{n_i} \in K^\times / \left( R^\times \right)^2,$$

où le déterminant est calculé en sur des $R$-bases de $\rho^{H_i}$.

**Remarque 3.4.14.** Comme précédemment, $\langle , \rangle$ peut être à valeurs dans n'importe quelle extension $L$ de $K$ et la classe de $C_\Theta(\rho)$ dans $K^\times / (R^\times)^2$ est indépendante du choix de $\langle , \rangle$.

**Exemple 3.4.15.**
1. Si $R = \mathcal{O}_K$ (où la caractéristique de $K$ est nulle) alors $\forall G$ si $\rho$ un $\mathcal{O}_K[G]$-module auto-dual, $C_\Theta(\rho)$ est bien définie comme élément de $K^\times / \left(\mathcal{O}_K^\times\right)^2$.
2. Si $R = K = k$ un corps fini de caractéristique $p$ alors si $p \nmid |G|$ et $\rho$ est un $k[G]$-module auto-dual, $C_\Theta(\rho)$ est bien définie comme élément de $k^\times / (k^\times)^2$.

**Proposition 3.4.16.** Soit $G$ un groupe fini, $K$ un corps local (extension finie de $\mathbb{Q}_p$), $\mathcal{O}_K$ son anneau des entiers et $\mathfrak{p}$ son unique idéal maximal. Si $\rho : G \longrightarrow GL(V) \simeq GL_n(K)$ une $K[G]$-représentation auto-duale et $p$ ne divise pas $|G|$ alors :

$$ord_\mathfrak{p} C_\Theta(\rho) \equiv 0 \mod 2$$

pour toute $G$-relation $\Theta$.

**Démonstration.** Après un changement de base éventuelle, $\rho$ est à valeurs dans $GL_n(\mathcal{O}_K)$ (voir le lemme 6.2.3). D'après la proposition 43 de [54], pour $p \nmid |G|$ , la théorie des représentations de $G$ sur $K$ est "la même" que celle sur $k_K$. En particulier, on a un accouplement non-dégénéré sur $k_K$ qui se relève en un accouplement $\langle , \rangle : T \times T \longrightarrow \mathcal{O}_K$ où $T$ est $\mathcal{O}_K[G]$-réseau de $V$. Si on prend cet accouplement $\langle , \rangle : T \times T \longrightarrow \mathcal{O}_K$ (qui se réduit donc en un accouplement non-dégénéré de $\bar{T} \times \bar{T} \longrightarrow k_K$ où $\bar{T}$ est un $k_K[G]$-module) pour calculer $C_\Theta(\rho)$, on obtient que $C_\Theta(\rho)$ est bien défini comme élément de $K^\times / \left(\mathcal{O}_K^\times\right)^2$ et que $C_\Theta(\rho \otimes k_K) \equiv C_\Theta(\rho \otimes K) \mod \mathfrak{p}_K$. Comme $C_\Theta(\rho \otimes k) \in k^\times$, on en déduit que $C_\Theta(\rho \otimes K) \notin \mathfrak{p}_K$ et $C_\Theta(\rho \otimes K)$ est une unité de $\mathcal{O}_K$ (à muliplication par un élement de $\left(\mathcal{O}_K^\times\right)^2$ près) donc de valuation triviale. Par conséquent, $ord_\mathfrak{p} C_\Theta(\rho) \equiv 0 \mod 2$. ■

**Définition 3.4.17.** Une fonction linéaire $\varphi$ sur l'anneau de Burnside de $G$ est une application de $\mathbb{Z}S$ dans un groupe abélien (noté multiplicativement) tel que $\varphi(\sum_i n_i H_i) = \prod_i \varphi(H_i)^{n_i}$. De plus, on dira que :
1. $\varphi$ est trivial sur $\Psi \in \mathbb{Z}S$ si $\varphi(\Psi) = 1$.
2. $\varphi \sim \varphi'$ si $\varphi/\varphi'$ est trivial sur toutes les $G$-relations.

**Définition 3.4.18.** Soit $G$ un groupe fini et $D$ un sous-groupe de $G$. Une fonction linéaire $\varphi$ sur l'anneau de Burnside de $G$ sera dite $D$-locale s'il existe une fonction linéaire $\varphi_D$ sur l'anneau de Burnside de $D$ telle que :

$$\varphi(H) = \varphi_D(\mathrm{Res}_D\, H) \left( = \prod_{x \in H\backslash G/D} \varphi_D(H^{x^{-1}} \cap D \right)$$

On notera $\varphi = (D, \varphi_D)$.

**Définition 3.4.19.** Soit $G$ un groupe fini, $D$ un sous-groupe de $G$ et $I$ un sous-groupe distingué de $D$ tel que $D/I$ est cyclique. Soit $\psi(e, f)$ une fonction de deux variables $e, f \in \mathbb{N}$. On définit :

$$(D, I, \psi) : H \to \prod_{x \in H\backslash G/D} \psi\left(\frac{|I|}{|H \cap I^x|}, \frac{[D : I]}{[H \cap D^x : I \cap I^x]}\right).$$

C'est une fonction $D$-locale sur l'anneau de Burnside de $G$, plus précisément

$$(D, I, \psi) = \left(D, U \to \psi\left(\frac{|I|}{|U \cap I|}, \frac{|D|}{|UI|}\right)\right).$$

**Théorème 3.4.20.** Soit $G$ un groupe fini, $D$ un sous-groupe de $G$ et $I$ un sous-groupe distingué de $D$ tel que $D/I$ est cyclique.

1. Si $\varphi = (D, \varphi_D)$ et $\varphi_D$ est trivial sur les $D$-relations alors $\varphi$ est trivial sur les $G$-relations.
2. Si $N \lhd G$ et $\varphi(H) = \varphi_{G/N}(HN/N)$ pour une application $\varphi_{G/N}$ sur l'anneau de Burnside de $G/N$ qui est trivial sur les $G/N$-relations alors $\varphi$ est trivial sur les $G$-relations.
3. Si $D_1 < D_2 < G$, $\varphi = (D_2, \varphi_2)$ et $\varphi_2 = (D_1, \varphi_1)$ alors $\varphi = (D_1, \varphi_1)$
4. Si $\psi(e, f)$ ne dépend pas de $e$ alors $(D, I, \psi) \sim 1$.
5. Si $I_0 \subset I$ est distingué dans $D$ tel que $D/I_0$ est cyclique et $\psi(e, f)$ est une fonction du produit $ef$ alors $(D, I, \psi) = (D, I_0, \psi)$.
6. Si $D_0$ est un sous-groupe de $D$ contenant $I$ et si pour $m$ divisant $f$ et $[D : D_0]$, on a $\psi(e, f) = \psi(e, f/m)^m$ alors $(D, I, \psi) = (D_0, I, \psi)$.
7. Soit $N \lhd G$ tel que $p \nmid [G : N]$. Soit $\varphi$ et $\phi$ deux applications sur les anneaux de Burnside de $G$ et $N$ respectivement alors :

$$\varphi = (N, \phi) \Longleftrightarrow \begin{cases} \varphi(H) = \prod\limits_{x \in G/D} \phi(H^x),\ H \subset N, \\ \varphi(H) = \phi(H \cap N) \text{ sinon.} \end{cases}$$

**Démonstration.** Voir le théorème 2.36 et le lemme 2.39 de [18]. ■

**Définition 3.4.21.** Pour une $K[G]$-représentation auto-duale $\rho$ munie d'un accouplement bilinéaire $\langle , \rangle$ non-dégénéré, $G$-invariant et à valeurs dans $K$, on définit :

$$\mathcal{D}_\rho : H \longrightarrow \det\left(\frac{1}{|H|} \langle , \rangle \Big| \rho^H\right) \in K^\times / K^{\times 2}.$$

**Remarque 3.4.22.**

1. $\mathcal{D}_\rho$ est bien défini (car $\langle , \rangle$ est $G$-invariant).
2. Si $\Theta$ est une $G$-relation alors $\mathcal{D}_\rho(\Theta) = C_\Theta(\rho)$.
3. Si $\mathcal{D}'_\rho$ est défini comme $\mathcal{D}_\rho$ mais pour un accouplement $\langle , \rangle'$ alors $\mathcal{D}_\rho \sim \mathcal{D}'_\rho$.
4. On a en particulier $\mathcal{D}_{\rho \oplus \rho'} \sim \mathcal{D}_\rho \mathcal{D}_{\rho'}$.

**Proposition 3.4.23.** Si $D < G$ et si $\rho$ est une $K[D]$-représentation auto-duale alors $\mathcal{D}_{Ind_D^G \rho} \sim (D, \mathcal{D}_\rho)$ comme fonctions à valeurs dans $K^\times / K^{\times 2}$.

**Démonstration.** Voir le lemme 2.43 de [18]. ■

**Proposition 3.4.24.** Soit $\rho$ est une $K[G]$-représentation auto-duale.

1. Si $G = G'/N$ et $\Theta$ est une $G$-relation alors si $\Theta'$ désigne le relèvement de $\Theta$ à $G'$ alors $C_\Theta(\rho) = C_{\Theta'}(\rho)$.
2. Si $G < G'$ et $\Theta$ est une $G'$-relation alors $C_\Theta(Ind_G^{G'} \rho) = C_{\mathrm{Res}_G \Theta}(\rho)$.
3. Si $D < G$ et $\Theta$ est une $D$-relation alors $C_\Theta(\mathrm{Res}_D \rho) = C_{Ind_D^G \Theta}(\rho)$.

**Démonstration.** Voir la proposition 2.45 de [18]. ■

**Lemme 3.4.25.** Si $H$ est un sous-groupe cyclique de $G$ alors $C_\Theta(K[G/H]) = 1$ pour toutes $G$-relations $\Theta$ (autrement dit, $\mathcal{D}_{K[G/H]} \sim 1$).

**Démonstration.** Voir le lemme 2.46 de [18]. ■

### 3.4.3 Signes locaux et nombres de Tamagawa.

Soit $K$ un corps local de caractéristique 0, $F/K$ une extension galoisienne de groupe $D$ et $A/K$ une variété abélienne principalement polarisée.

**Théorème 3.4.26.** Supposons que l'une des quatre conditions suivantes est vérifiée :

1. $D$ est cyclique.
2. $A = E$ est une courbe elliptique semi-stable.
3. $A = E$ est une courbe elliptique à réduction additive et la caractéristique résiduelle de $K$ est $l > 3$.
4. $A$ a réduction semi-stable.

alors il existe un $\mathbb{Q}D$-module $\mathcal{V}$ tel que :

1. $\frac{W(A/K,\tau)}{W(\tau)^{2\dim A}} = (-1)^{\langle \mathcal{V},\tau\rangle}$ pour toute représentation auto-duale $\tau$.
2. $C_v \sim \mathfrak{D}_{\mathcal{V}}$.
   où $\mathfrak{D}_{\mathcal{V}}(\Theta) = C_\Theta(\mathcal{V})$ et $C_v(\Theta) = \prod_i C_v(H_i)^{n_i}$ avec $C_v(H_i)^{n_i} = c_w(E/L^{H_i})\omega(H_i)$, $c_w(E/L^{H_i})$ est le nombre de Tamagawa local et $\omega(H_i) = \left| \frac{\omega^0_{E/K_v}}{\omega^0_{E/\left(L^{H_i}\right)_w}} \right|_{\left(L^{H_i}\right)_w}$ où $\omega^0_{E/K_v}$ est une différentielle invariante minimale).

**Démonstration.** Voir le théorème 3.2 de [18]. ■

**Remarque 3.4.27.** On remarquera que pour le cas d'une courbe elliptique, la formule $\frac{W(A/K,\tau)}{W(\tau)^{2\dim A}} = (-1)^{\langle \mathcal{V},\tau\rangle}$ est précisément de la forme des formules de Rohrlich.

**Corollaire 3.4.28.** Si $\Theta$ est une $D$-relation et $p$ est un nombre premier ($p \neq 2$ dans le cas 4) alors :

$$ord_p C_\Theta(\mathcal{V}\otimes\mathbb{Q}_p) \equiv ord_p C_v(\Theta) \mod 2.$$

**Remarque 3.4.29.** Au chapitre 5, nous montrerons une congruence similaire pour une représentation modérément ramifiée du groupe de Weil.

**Corollaire 3.4.30.** Si $\Theta$ est une $D$-relation et $p$ est un nombre premier ($p \neq 2$ dans le cas 4) alors :

$$\forall \tau \in T_{\Theta,p},\ W(A/K,\tau) = (-1)^{ord_p C_v(\Theta)}$$

où $T_{\Theta,p} = \left\{ \begin{array}{l|l} \sigma \text{ une } \overline{\mathbb{Q}}_p[G]\text{-représentation} & \langle \sigma,\rho\rangle \equiv ord_p C_\Theta(\rho) \pmod 2 \\ \text{auto-duale} & \forall \rho \text{ une } \mathbb{Q}_p[G]\text{-representation auto-duale} \end{array} \right\}$

Par ailleurs, on a le théorème global suivant :

**Théorème 3.4.31.** Soit $L/K$ une extension de galoisienne de corps de nombres de groupe de galois $G := G_{L/K}$, $p$ un nombre premier et $\Theta = \sum_i n_i H_i$ une $G$-relation. Pour toute courbe elliptique $E/K$, la représentation $S_p(E/K)$ est auto-duale et :

$$\langle \tau, S_p(E/K)\rangle \equiv ord_p\left(C(\Theta)\right) \mod 2$$

où $C(\Theta) = \prod_i (C_{E/L^{H_i}})^{n_i}$, $C_{E/L^{H_i}} = \prod_v C_{w|v}(H^i) = \prod_v \prod_{w|v} C_w(H_i)$.

**Démonstration.** Voir le théorème 1.14 de [18]. ■

**Remarque 3.4.32.** Le même résultat est valable pour une variété abélienne principalement polarisée $A/K$, sauf dans le cas où $p = 2$ où il faut supposer en plus que la polarisation provient d'un diviseur $K$-rationnel.

En combinant les deux résultats précédents, on obtient les résultats suivants concernant la conjecture de $p$-parité (avec un twist) :

**Théorème 3.4.33.** Soit $L/K$ une extension de galoisienne de corps de nombres. Si $E/K$ est une courbe elliptique dont les places de réduction additive au-dessus de 2 et 3 ont un groupe de décomposition cyclique alors pour tout $p$ premier et toute $G_{L/K}$-relation $\Theta$ on a :

$$(-1)^{\langle \tau, S_p(E/K)\rangle} = W(E/K, \tau) \text{ pour } \tau \in T_{\Theta,p}$$

**Théorème 3.4.34.** Soit $p$ premier, $p > 2$ et $L/K$ une extension de galoisienne de corps de nombres. Si $A/K$ une variété abélienne dont les places de réduction additive ont un groupe de décomposition cyclique alors pour toute $G_{L/K}$-relation $\Theta$ on a :

$$(-1)^{\langle \tau, S_p(A/K)\rangle} = W(A/K, \tau) \text{ pour } \tau \in T_{\Theta,p}.$$

Au chapitre 6 à l'aide des résultats obtenus sur les représentations modérément ramifiées du groupe de Weil nous pourrons démontrer le résultat suivant :

**Théorème 3.4.35.** Soient $p$ premier, $p > 2d + 1$ et $L/K$ une extension galoisienne de corps de nombres. Soit $A/K$ une variété abélienne de dimension $d$, on suppose que les places finies suivantes ont un groupe de décomposition cyclique :
· les places $v$ de réduction additive, au-dessus des nombres premiers inférieurs ou égaux à $2d + 1$.
· les places $v$ où $A$ n'a pas réduction semi-stable et $A$ a mauvaise réduction sur l'extension modérément ramifiée maximale de $K_v$.
· les places $v \mid p$ (si $p$ n'est pas une place de réduction semi-stable)
Alors pour toute $G_{L/K}$-relation $\Theta$ on a :

$$(-1)^{\langle \tau, S_p(A/K)\rangle} = W(A/K, \tau) \text{ pour } \tau \in T_{\Theta,p}.$$

# Chapitre 4

# Invariance de la conjecture de parité pour les p-groupes de Selmer d'une courbe elliptique par une $D_{2p^n}$-extension

Ce chapitre est une traduction française de l'article "Invariance of the parity conjecture for $p$-Selmer groups of elliptic curves in a $D_{2p^n}$-extension" paru au Bulletin de la SMF (voir [10]). On remarquera quelques redondances avec les chapitres précédents, on a choisi de laisser l'article intacte (mis à part la traduction et quelques références) pour la commodité du lecteur qui serait intéressé par cette seule partie.

**Résumé 4.0.36.** Dans la section 2, on démontre un résultat de $p$-parité, dans une extension galoisienne de corps de nombre de groupe $D_{2p^n}$, pour le twist $1 \oplus \eta \oplus \tau$ :

$$W(E/K, 1 \oplus \eta \oplus \tau) = (-1)^{\langle 1 \oplus \eta \oplus \tau, X_p(E/L) \rangle},$$

où $E$ est une courbe elliptique définie sur $K$, $\eta$ et $\tau$ sont respectivement le caractère quadratique et une représentation irréductible de degré 2 de $Gal(L/K) = D_{2p^n}$, et $X_p(E/L)$ est le $p$-groupe de Selmer. La principale nouveauté est qu'on utilise un résultat de congruence (du à Deligne) pour déterminer les "root numbers" locaux dans les mauvais cas (les places additives au-dessus de 2 et 3). On donne aussi, en utilisant la machinerie des frères Dokchitser, deux applications à la conjecture de $p$-parité.

## 4.1 Introduction

### 4.1.1 La conjecture de Birch-Swinnerton-Dyer et la conjecture de parité

Soit $K$ un corps de nombres et $E$ une courbe elliptique sur $K$. Notons $K_v$ la complétion de $K$ à la place $v$.

On rappelle quelques définitions :

**Définition 4.1.1.** (Module de Tate) :
Le module de Tate $l$-adique de $E$ est la limite projective du système formé par les applications de multiplication par $l$, $E[l^{n+1}] \longrightarrow E[l^n]$, où $E[m]$ est le noyau de la multiplication

par $m$ sur $E$. Posons

$$T_l(E) = \varprojlim E[l^n], V_l(E) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(E)$$

et :

$$\sigma'_{E/K_v,l} : Gal(\overline{K}_v/K_v) \longrightarrow GL(V_l(E)^*).$$

Fixons un plongement, $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$ ; on peut alors associer à $\sigma'_{E/K_v,l}$ une représentation complexe $\sigma'_{E/K_v,l,\iota}$ du groupe de Weil-Deligne (voir la section 1.3.3).

**Remarque 4.1.2.** On peut montrer que la classe d'isomorphie de $\sigma'_{E/K_v} := \sigma'_{E/K_v,l,\iota}$ est indépendante du choix de $l$ et de $\iota$ (voir l'exemple 1.3.26).

Notons $L(E/K, s)$ la fonction $L$ globale, produit des fonctions $L$ locales :

$$L(E/K, s) = \prod_{v \text{ finies}} L(E/K_v, s) \left( = \prod_{v \text{ finies}} L(\sigma'_{E/K_v}, s) \right)$$

définie pour $\mathrm{Re}(s) > \dfrac{3}{2}$ (voir la section 2.2 pour le lien avec la définition classique de $L(E/K_v, s)$ et celle utilisant $\sigma'_{E/K_v}$) et par

$$\Lambda(E/K, s) = A(E/K)^{s/2} L(E/K, s)(2(2\pi)^{-s}\Gamma(s))^{[K:\mathbb{Q}]},$$

la fonction $L$ complète où $A(E/K)$ est une constante qui s'exprime en fonction du discriminant et du conducteur de $E/K$ (voir le chapitre 3).

Rappellons les conjectures classiques suivantes :

**Conjecture 4.1.3.** (Birch et Swinnerton-Dyer : BSD) :

$$ord_{s=1}\Lambda(E/K, s) = rk(E/K).$$

**Conjecture 4.1.4.** (Equation fonctionnelle de $\Lambda$ : FE) :
$L(E/K, s)$ admet un prolongement holomorphe à $\mathbb{C}$ et il existe un signe

$$W(E/K) = \prod_v W(E/K_v) \in \{\pm 1\}$$

tel que :

$$\Lambda(E/K, s) = W(E/K)\Lambda(E/K, 2 - s)$$

(voir la section 2.4 et notamment l'exemple 2.4.15 $W(E/K_v) := W(\sigma'_{E/K_v})$ et le chapitre 3 pour l'équation fonctionnelle de $\Lambda$).

Cette conjecture est connue dans quelques cas :
- Pour les courbes elliptiques sur $\mathbb{Q}$ grâce aux résultats de modularité dus à Wiles, Taylor, Breuil, Diamond et Conrad.
- Pour les courbes elliptiques sur un corps de nombres totalement réel, on sait que $\Lambda$ admet un prolongement méromorphe et satisfait l'équation fonctionnelle grâce à un résultat de modularité potentiel de Wintenberger (voir [64]) joint à un argument de Taylor.

Dans le cas général, la Conjecture 4.1.4 n'est pas connue.
La conjecture de Birch et Swinnerton-Dyer implique la conjecture plus faible suivante :

**Conjecture 4.1.5.** (BSD (mod 2))

$$rg(E/K) \equiv ord_{s=1}\Lambda(E/K,s) \,(\mathrm{mod}\, 2)\,.$$

Combinée avec l'équation fonctionnelle conjecturale on obtient :

**Conjecture 4.1.6.** (Conjecture de parité)

$$(-1)^{rg(E/K)} = W(E/K).$$

Tim et Vladimir Dokchitser ont montré que cette conjecture est vrai si on suppose que la partie de $6^\infty$-torsion du groupe de Tate-Shafarevich de $E$ sur $K(E[2])$ est finie (voir [21] Th 7.1 p.20).

**Définition 4.1.7.** Groupe de Selmer :
Soit

$$X_p(E/K) := Hom_{\mathbb{Z}_p}(S(E/K,p^\infty), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

où $S(E/K,p^\infty) := \varinjlim_n S(E/K,p^n)$ est le $p^\infty$-groupe de Selmer, qui apparaît dans la suite exacte suivante :

$$0 \longrightarrow E(K)\otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow S(E/K,p^\infty) \longrightarrow Ш_{E/K}[p^\infty] \longrightarrow 0.$$

Si on pose $\mathrm{rg}_p(E/K) := \dim_{\mathbb{Q}_p} X_p(E/K) = rg(E/K) + \mathrm{cork}_{\mathbb{Z}_p} Ш_{E/K}[p^\infty]$, on a la version plus accessible suivante de la conjecture 4.1.6 :

**Conjecture 4.1.8.** ($p$-parity conjecture)

$$(-1)^{\mathrm{rg}_p(E/K)} = W(E/K).$$

Si $L/K$ est une extension galoisienne finie et $\tau$ est une $\overline{\mathbb{Q}}_p$-représentation auto-duale de $Gal(L/K)$ alors on peut énoncer une version équivariante de la conjecture 4.1.8 :

**Conjecture 4.1.9.** (Conjecture de $p$-parité avec twist (auto-duale))

$$(-1)^{\langle \tau, X_p(E/L)\rangle} = W(E/K,\tau),$$

où $W(E/K,\tau) = \prod_v W(\sigma'_{E/K_v} \otimes \mathrm{Res}_{D_v}\tau)$, $D_v \subset Gal(L/K)$ est le groupe de décomposition en $v$ et $\langle \tau, * \rangle$ est le produit scalaire classique des caractères de $\tau$ et du complexifié de $*$

C'est cette dernière conjecture dans un cas particulier qui va nous intéresser pour le reste du chapitre.

### 4.1.2 Enoncé du théorème principal et applications à la conjecture de $p$-parité

Soit $K$ un corps de nombres, $E/K$ une courbe elliptique et $L/K$ une extension galoisienne finie tel que $Gal(L/K) \simeq D_{2p^n}$, avec $p \geq 5$ un nombre premier.

$D_{2p^n}$ admet les représentations irréductible suivantes sur $\overline{\mathbb{Q}}_p$ :
- 1 la représentation triviale.
- $\eta$ le caractère quadratique.
- $\frac{p^n-1}{2}$ représentations irreducibles de degré 2 ; elles sont de la forme,

$$I(\chi) := Ind_{C_{p^n}}^{D_{2p^n}}(\chi) = I(\chi^{-1}),$$

où $\chi$ est un caractère non-trivial de $C_{p^n}$ ($I(1) = 1 \oplus \eta$ est réductible).
Voir par exemple §5.3 p.52 de [54] pour une description des représentations irréductibles de $D_{2p^n}$.

Soit $\tau = I(\chi)$ une représentation irréductible de degré 2 de cette forme.

**Théorème 4.1.10.** Avec les notations ci-dessus et $p \geq 5$, on a l'équalité suivante :

$$\frac{W(E/K, \tau)}{W(E/K, 1 \oplus \eta)} = \frac{(-1)^{\langle \tau, X_p(E/L)\rangle}}{(-1)^{\langle 1 \oplus \eta, X_p(E/L)\rangle}}$$

Autrement dit, la conjecture de $p$-parité pour $E/K$ tensorisé par $1 \oplus \eta \oplus \tau$ est vérifiée :

$$W(E/K, 1 \oplus \eta \oplus \tau) = (-1)^{\langle 1 \oplus \eta \oplus \tau, X_p(E/L)\rangle}$$

**Remarque 4.1.11.** Les frères Dokchitser ont montré que cette égalité est vérifiée dans deux cas :
• *Le cas où $p$ est un nombre premier mais l'extension $L/K$ admet un groupe de décomposition cyclique en toute place de réduction additive de $E/K$ au-dessus de* 2 *et* 3 (voir le théorème 4.2 (1) p.65 de [18] ).

• *Le cas où* $p \equiv 3 \pmod 4$ *(sans conditions supplémentaires) en utilisant un résultat global fort concernant la conjecture de p-parité sur les corps de nombres totalement réel dû à Jan Nekovář dans [36]* (voir la proposition 6.12 p.18 de [21]).
· Dans ce chapitre, on prouve l'égalité pour tout $p \geq 5$ (sans conditions supplémentaires).

**Remarque 4.1.12.** L'énoncé du théorème 4.1.10 reste valable pour $p = 3$ (voir la remarque ci-dessus). Ce cas peut être prouvé sans "les douloureux calculs" ([18] p.53) dans le cas de la réduction additive (voir l'appendice à ce chapitre).

**Corollaire 4.1.13.** $\dfrac{W(E/K, I(\chi))}{(-1)^{\langle I(\chi), X_p(E/L)\rangle}}$ ne dépend pas de $\chi : C_{p^n} \longrightarrow \mathbb{C}^*$.

Le théorème 4.1.10 est équivalent au fait que l'hypothèse 4.1 de [18] soit vérifiée pour toute courbe elliptique et tout nombre premier $p > 3$ (d'après la remarque 4.1.11 ci-dessus le résultat est aussi vrai pour $p = 3$). Maintenant, en utilisant la machinerie des frères Dokchitser (voir les théorèmes 4.3 et 4.5 de [18]), nous obtenons les théorèmes suivants :

**Théorème 4.1.14.** Soit $K$ un corps de nombres, $p \geq 3$, et $E/K$ une courbe elliptique. Supposons que $F$ est une $p$-extension de l'extension galoisienne $M/K$, galoisienne sur $K$. Si la conjecture de $p$-parité

$$(-1)^{rg_p E/L} = W(E/L)$$

est vérifiée pour tout sous-corps $K \subset L \subset M$, alors elle est vérifiée pour tout sous-corps $K \subset L \subset F$.

**Théorème 4.1.15.** Soit $K$ un corps de nombres, $p \geq 3$, $E/K$ une courbe elliptique et $F/K$ une extension galoisienne. Supposons que le $p$-sous-groupe de $P$ de $G = Gal(F/K)$ est distingué et que $G/P$ est abélien. Si la conjecture de $p$-parité est vérifiée pour $E$ sur $K$ et ses extensions quadratiques dans $F$, alors elle est vérifiée pour tout twists de $E$ par une représentation orthogonale de $G$.

## 4.2 Invariance de la conjecture de parité dans une $D_{2p^n}$-extension

### 4.2.1 Réduction au cas d'une $D_{2p}$-extension

On réduit la démonstration du théorème 4.1.10 grâce à l'utilisation de l'induction combiné avec la propriété d'invariance galoisienne des signes locaux dû à Rohrlich (voir le théorème 2 de [47]), à la proposition suivante :

**Proposition 4.2.1.** Il suffit de prouver le théorème 4.1.10 dans le cas où $n = 1$ (i.e. $Gal(L/K) \simeq D_{2p}$).

**Démonstration.** Supposons que le théorème 4.1.10 est vrai pour $n = N - 1$. On va montrer que le théorème est vrai pour $n = N$.
Considérons l'extension galoisienne finie $L/K$ tel que $Gal(L/K) \simeq D_{2p^N}$ et $\tau = I(\chi)$ est une réprésentation irréductible de degré 2 de $D_{2p^N}$.

1. Si $\chi$ n'est pas injective, alors le résultat est connu par hypothèse de récurrence.
2. Si $\chi$ est injective. Soit $\sigma = res(I(\chi)) := res^{D_{2p^N}}_{D_{2p^{N-1}}}(I(\chi))$ alors

$$\sigma = I(\chi'), \text{ où } \chi' := \chi_{\big|_{C_{p^{N-1}}}} : C_{p^{N-1}} \to \overline{\mathbb{Q}}_p \text{ est injective.}$$

On a $Ind^{D_{2p^N}}_{D_{2p^{N-1}}}(\sigma) = \bigoplus_{\chi_0} I(\chi_0)$, où la somme est prise sur les $\chi_0$ tel que $\chi_{0\big|_{C_{p^{N-1}}}} = \chi_{\big|_{C_{p^{N-1}}}}$.
Pour chaque tel $\chi_0$ il y a un élement de $Aut(\mathbb{C})$ qui envoi $\chi$ sur $\chi_0$ et $I(\chi)$ sur $I(\chi_0)$ et par l'inductivité des signes locaux dans les extensions galoisiennes :

$$W(E/K, \sigma) = W(E/K, Ind^{D_{2p^N}}_{D_{2p^{N-1}}}(\sigma)).$$

Puis par l'invariance galoisienne des signes locaux (voir le théorème 2 de [47]) :

$$W(E/K, I(\chi')) = W(E/K, I(\chi_0)), \forall \chi_0 \text{ tel que } \chi_{0|_{C_{p^{N-1}}}} = \chi_{|_{C_{p^{N-1}}}}$$

donc $W(E/K, \sigma) = W(E/K, Ind^{D_{2p^N}}_{D_{2p^{N-1}}}(\sigma)) = W(E/K, \tau)^p = W(E/K, \tau)$.
Par ailleurs,

$$\langle \sigma, X_p(E/L) \rangle = \left\langle Ind^{D_{2p^N}}_{D_{2p^{N-1}}}(\sigma), X_p(E/L) \right\rangle = p. \langle \tau, X_p(E/L) \rangle ,$$

car $X_p(E/L)$ est une $\mathbb{Q}_p$-représentation et par conséquent

$$(-1)^{\langle 1 \oplus \eta \oplus \sigma, X_p(E/L) \rangle} = (-1)^{\langle 1 \oplus \eta \oplus \tau, X_p(E/L) \rangle}.$$

Enfin, par hypothèse de récurrence, $(-1)^{\langle 1 \oplus \eta \oplus \sigma, X_p(E/L) \rangle} = W(E/K, \sigma)$ et on en déduit que,

$$W(E/K, 1 \oplus \eta \oplus \tau) = (-1)^{\langle 1 \oplus \eta \oplus \tau, X_p(E/L) \rangle}.$$

■

### 4.2.2 Le cas d'une $D_{2p}$-extension

Commençons par réénoncer le théorème 4.1.10 dans le cas d'une $D_{2p}$-extension.

Soit $K$ un corps de nombres, $E/K$ une courbe elliptique et $L/K$ une extension galoisienne tel que $Gal(L/K) \simeq D_{2p} \simeq C_p \rtimes C_2$, où $p \geq 5$ est un nombre premier. On va utiliser la notation $D_2$ au lieu de $C_2$ pour éviter les confusions avec les facteurs de Tamagawa locaux $C_v$.

Rappelons que les représentations irréductibles de $D_{2p}$ sur $\overline{\mathbb{Q}}_p$ sont :
- 1 la représentation trivial.
- $\eta$ le caractère quadratique.
- $I(\chi) = Ind_{C_p}^{G}(\chi)$ les représentations irréductibles de degré 2, où $\chi$ est un caractère non-trivial de $C_p$.

**Théorème 4.2.2.** Avec les notations ci-dessus et $p \geq 5$, on a l'égalité suivante :

$$\frac{W(E/K,\tau)}{W(E/K,1\oplus\eta)} = \frac{(-1)^{\langle\tau,X_p(E/L)\rangle}}{(-1)^{\langle 1\oplus\eta,X_p(E/L)\rangle}}.$$

Autrement dit, la conjecture de $p$-parité conjecture pour $E/K$ tensorisée par $1\oplus\eta\oplus\tau$ est vérfiée :

$$W(E/K,1\oplus\eta\oplus\tau) = (-1)^{\langle 1\oplus\eta\oplus\tau,X_p(E/L)\rangle}.$$

La démonstration du théorème 4.2.2 nous occupera le reste de la section 4.2.

On utilise les notations suivantes :
- $v$ une place finie de $K$.
- $K_v$ le complété de $K$ en $v$.
- $q = l_v^r$ le cardinal du corps résiduel de $K_v$.
- $z \mid v$ une place finie de $L$.
- $w \mid v$ une place finie de $L^H$ (où $H$ est un sous-groupe de $Gal(L/K) = D_{2p}$).
- $\delta = ord_v$ (le discriminant minimal de $E/K_v$).
- $\delta_H = ord_w\left(\text{le discriminant minimal de } E/\left(L^H\right)_w\right)$.
- $e_H$ le degré de ramification de $\left(L^H\right)_w/K_v$.
- $f_H$ le degré résiduel de $\left(L^H\right)_w/K_v$.
- $\omega^0_{E/K_v}$ = une differentielle invariante minimale de $E/K_v$.
- $C_w(E/L^H) = c_w(E/L^H)\omega(H)$,

où $\begin{cases} c_w(E/L^H) = \text{ facteur de Tamagawa local de } E/\left(L^H\right)_w, \\ \omega(H) = \left|\frac{\omega^0_{E/K_v}}{\omega^0_{E/(L^H)_w}}\right|_{(L^H)_w}. \end{cases}$

Une differentielle invariante minimale de $E/K_v$ et une de $E/\left(L^H\right)_w$ diffèrent par un élément de $\left(L^H\right)_w$. Si on choisit $\omega'^0_{E/K_v}$ (resp $\omega'^0_{E/(L^H)_w}$) une differentielle invariante minimale différente de $E/K_v$ (resp $E/\left(L^H\right)_w$), on a $\frac{\omega'^0_{E/K_v}}{\omega'^0_{E/(L^H)_w}} = \alpha\frac{\omega^0_{E/K_v}}{\omega^0_{E/(L^H)_w}}$, où $\alpha$ est une unité de $\left(L^H\right)_w$ (voir [59] p.172). Par conséquent, $\omega(H)$ est bien défini.

De plus, si $l_v > 3$ alors (voir [18] p.53) :

$$\left|\frac{\omega^0_{E/K_v}}{\omega^0_{E/(L^H)_w}}\right|_{(L^H)_w} = q^{\frac{\delta.e_H-\delta_H}{12}f_H}$$
$$\left(= q^{\left\lfloor\frac{\delta.e_H}{12}\right\rfloor f_H} \text{ dans le cas de la potentiellement bonne réduction}\right).$$

Pour $D_{2p}$, on a l'égalité suivante : $Ind_{\{1\}}^{D_{2p}}1 - 2.Ind_{D_2}^{D_{2p}}1 - Ind_{C_p}^{D_{2p}}1 + 2.1 = 0$ entre représentations virtuelles de $G$. Cela donne une $G$-relation $\Theta : \{1\} - 2D_2 - C_p + 2G$ (voir la définition 3.4.2).

On rappelle deux définitions dans notre cadre (i.e. avec $\Theta : \{1\} - 2D_2 - C_p + 2D_{2p}$), pour les définitions générales voir la section 3.4.2.

**Définition 4.2.3.** Soit $\rho$ une $\mathbb{Q}_p[G]$-representation auto-duale.
Choissisons une application $\mathbb{Q}_p$-bilinéaire non-dégénérée $G$-invariante $\langle,\rangle$ sur $\rho$ et posons

$$C_\Theta(\rho) = \det(\langle,\rangle\left|\rho^{\{1\}}\right.)\det(\tfrac{1}{2}\langle,\rangle\left|\rho^{D_2}\right.)^{-2}\det(\tfrac{1}{p}\langle,\rangle\left|\rho^{C_p}\right.)^{-1}\det(\tfrac{1}{2p}\langle,\rangle\left|\rho^{D_{2p}}\right.)^2$$

appartenant à $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, où $\det(\langle,\rangle\left|\rho^A\right.)$ est $\det((\langle e_i,e_j\rangle)_{i,j})$ dans n'importe quelle $\mathbb{Q}_p$-base $\{e_i\}$ of $\rho^A$.

**Remarque 4.2.4.** $C_\Theta(\rho)$ est bien défini et ne dépend pas du choix de l'application bilinéaire (voir la remarque 1 et le théorème 2.17 p37 de [18]).

**Définition 4.2.5.** On définit :

$$T_{\Theta,p} = \left\{ \begin{array}{l|l} \sigma \text{ une } \overline{\mathbb{Q}}_p[G]\text{-rep} & \langle\sigma,\rho\rangle \equiv ord_p C_\Theta(\rho) \pmod 2 \\ \text{auto-duale} & \forall\rho \text{ une } \mathbb{Q}_p[G]\text{-rep auto-duale} \end{array} \right\}$$

On suit la démarche des frères Dokchitser et on a le théorème suivant :

**Théorème 4.2.6.** (Théorème 1.14 de [18]). Soit $L/K$ une extension galoisienne de groupe de Galois $G = D_{2p}$, où $p > 2$ est un nombre premier. Soit $\Theta : \{1\} - 2D_2 - C_p + 2D_{2p}$. Pour toute courbe elliptique $E/K$, la $\mathbb{Q}_p[G]$-représention $X_p(E/L)$ est auto-duale, et

$$\forall\sigma \in T_{\Theta,p}, \quad (-1)^{\langle\sigma,X_p(E/L)\rangle} = (-1)^{ord_p(C)},$$

où $C = \prod_{v\nmid\infty} C_v$ avec $C_v = C_v(\{1\})C_v(D_2)^{-2}C_v(C_p)^{-1}C_v(G)^2$
et $C_v(H) = \prod_{\substack{w|v \\ w \text{ places of } L^H}} C_w(E/L^H)$.

Maintenant, comme $1\oplus\eta\oplus\tau \in T_{\Theta,p}$ (voir [18], exemple 2.53 p.46), on doit simplement montrer que :

$$\frac{W(E/K,\tau)}{W(E/K,1\oplus\eta)} = (-1)^{ord_p C}. \tag{4.1}$$

De plus, comme on est seulement intéressé par la parité de $ord_p(C)$, il n'est pas néccéssaire de déterminer $C_v(D_2)$ et $C_v(G)$, car ces termes n'apportent qu'une contribution paire (car ils apparaissent avec un exposant pair).

Les deux membres de l'égalité (4.1) sont de nature locale.

Comme $W(E/K,\tau) = \prod_v W(E/K_v,\tau_v)$, où $\sigma_v := res_{Gal(L_z/K_v)}\sigma$, il nous suffit de démontrer l'égalité locale suivante :

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = (-1)^{ord_p(C_v)}, \tag{4.2}$$

pour toute place finie $v$ of $K$ ($v \mid \infty$ ne contribue pas, car $p \neq 2$).

Notons $G_v := Gal(L_z/K_v)$ le groupe de décomposition de $v$. La démonstation du théorème 4.2.2 se décompose en plusieurs cas :

- $G_v = \{1\}$ (il y a $2p$ places au-dessus de $v$ dans $L$) voir section A
- $G_v = D_2$ (il y a $p$ places au-dessus de $v$ dans $L$) voir section B
- $G_v = C_p$ (il y a 2 places au-dessus de $v$ dans $L$) voir section A
- $G_v = D_{2p}$ (il y a une unique place au-dessus de $v$ dans $L$) voir section C

On commence par rappeler quelques propriétés des facteurs de Tamagawa locaux d'une courbe elliptique.

**Facteurs de Tamagawa locaux d'une courbe elliptique**

On conserve les notations et les hypothèses ci-dessus.

Le facteur de Tamagawa local en $v$, $c(E/K_v) = \#\left(E(K_v)/E^0(K_v)\right)$, où $E^0(K_v)$ est l'ensemble des points de réduction non-singulière (voir le début du chapitre 6 et la proposition 6.1.5). le facteur $c(E/K_v)$ est déterminé par l'algorithme de Tate (voir [58] IV §9) :

$$c(E/K_v) = \begin{cases} 1 & \text{si } E \text{ a bonne réduction en } v, \\ 1,\ 2,\ 3 \text{ ou } 4 & \text{si } E \text{ a réduction additive en } v, \\ n & \text{si } E \text{ a réduction multiplicative déployée} \\ & \text{de type } I_n \text{ en } v, \\ 1 \text{ ou } 2 & \text{si } E \text{ a réduction multiplicative non-déployée} \\ & \text{de type } I_n \text{ en } v. \end{cases}$$

Si $E$ acquiert réduction semi-stable sur $L_z$, alors :

1. Si $E$ a réduction multiplicative déployée de type $I_n$ sur $K_v$, alors : $c(E/\left(L^H\right)_w) = n.e_H$.
2. Si $E$ a réduction multiplicative non-déployée de type $I_n$ sur $K_v$, alors :
$$c(E/\left(L^H\right)_w) = \begin{cases} n.e_H & \text{si } E \text{ a réduction multiplicative déployée} \\ & \text{sur } \left(L^H\right)_w, \\ 1 \text{ ou } 2 & \text{sinon.} \end{cases}$$
3. Si $E$ a potentiellement bonne réduction, alors $c(E/\left(L^H\right)_w) = 1, 2, 3$ ou $4$.
4. Si $E$ a réduction additive et potentiellement multiplicative alors :
$$c(E/\left(L^H\right)_w) = \begin{cases} n.e_H & \text{si } E \text{ a réduction multiplicative déployée} \\ & \text{de type } I_n \text{ sur } \left(L^H\right)_w \text{ et } l_v \neq 2, \\ 1, 2, 3 \text{ ou } 4 & \text{sinon.} \end{cases}$$

La proposition suivante sera utile dans les calculs à venir.

**Proposition 4.2.7.** 1. Si $w_1$ et $w_2$ sont deux places de $L$ au-dessus du même $v$, alors $c_{w_1}(E/L) = c_{w_2}(E/L)$ et en particulier :

$$\begin{cases} C_v(\{1\}) = C_w(E/L)^r, \\ C_v(C_p) = C_{w'}(E/L^{C_p})^{r'}, \end{cases}$$

où $r$ =le nombre de places $w$ de $L$ tel que $w \mid v$ et $r'$ =le nombre de places $w'$ de $L^{C_p}$ tel que $w' \mid v$.

2. Si $E/K$ a potentiellement bonne réduction en $v$, alors :
Pour toutes places $w$ (resp. $w'$) de $L$ (de $L^{C_p}$)

$$c_w(E/L)(\text{resp. } c_{w'}(E/L^{C_p})) \in \{1, .., 4\},$$

et par conséquent

$$ord_p(c_v) = 0 \text{ et } (-1)^{ord_p(C_v)} = (-1)^{ord_p\left(\frac{\omega(\{1\})}{\omega(C_p)}\right)}.$$

3. Si la réduction de $E/K$ en $v$ est semi-stable, alors pour tous sous-groupes $H$ de $D_{2p}$, $\delta_H = \delta.e_H$ et par conséquent $\omega(H) = 1$ et $(-1)^{ord_p(C_v)} = (-1)^{ord_p(c_v)}$.
4. Si $v \nmid p$ (i.e. $p \neq l_v$, $p$ est fixé, $l_v$ est variable), alors

$$ord_p(\omega(H)) = 0 \text{ et } (-1)^{ord_p(C_v)} = (-1)^{ord_p(c_v)}.$$

**Remarque 4.2.8.** D'après les points 3 et 4 de la proposition précédente, si $E/K$ a bonne réduction en $v$, alors $(-1)^{ord_p(C_v)} = 1$.
Dans le cas de bonne réduction en $v$, on a l'égalité (4.2) car dans ce cas $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = \frac{\det\tau_v(-1)}{\det(1\oplus\eta)_v(-1)} = 1$

**Remarque 4.2.9.** D'après les points 2 et 4, on déduit que le seul cas qui nécessite le calcul à la fois de $\omega(H)$ et de $c_w(E/L^H)$ est le cas de la réduction additive potentiellement multiplicative en $v \mid p$.

### A Les cas $G_v = \{1\}$ et $G_v = C_p$

Dans ces cas, $C_v(\{1\})$ et $C_v(C_p)$ sont des carrés, donc $ord_p(C_v) \equiv 0 \pmod 2$.
• Si $G_v = \{1\}$, $res_{Gal(L_z/K_v)}\tau = 1 \oplus 1 = (1 \oplus \eta)_v$, alors $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1$.
• Si $G_v = C_p$, $(1 \oplus \eta)_v = 1 \oplus 1$ et $\tau_v = \chi \oplus \chi^*$, alors

$$W(E/K_v, \tau_v) = 1 = W(E/K_v, (1 \oplus \eta)_v) \text{ (voir [18] lemma A.1 p.69).}$$

Dans les deux cas, on a donc : $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1 = (-1)^{ord_p(C_v)}$.

### B Le cas $G_v = D_2$

On a $\tau_v = (1 \oplus \eta)_v$, donc $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1$.

Par ailleurs, dans ce cas, pour toutes places $w' \mid v$ de $L^{C_p}$ et toute place $w \mid w'$ de $L$, $[\left(L^{C_p}\right)_{w'} : K_v] = 2$ et $\left(L^{C_p}\right)_{w'} = L_w$. En particulier, $C_v(\{1\}) = C_v(C_p)^p$, par conséquent $C_v = C_v(C_p)^{p-1}$ et $ord_p(C_v) = 0$.

Finalement, on obtient : $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1 = (-1)^{ord_p(C_v)}$.

## C Le case $G_v = D_{2p}$

Notons $w$ (resp $z$) l'unique place de $L^{C_p}$ (resp $L$) au-dessus de $v$.
Dans ce cas, il y a deux possibilités pour le groupe d'inertie de $G_v$, $I_v = C_p$ ou $D_{2p}$ (car $I_v$ est un sous-groupe distingué de $G_v = D_{2p}$ et $G_v/I_v$ est cyclique).
De plus, si $l_v \neq p$ alors $I_v = C_p$ :

· Si $l_v \neq 2$, simplement car le groupe d'inertie d'une extension modérément ramifiée est cyclique.

· Si $l_v = 2$, car le cas $I_v = D_{2p}$, $I_v^{wild} = D_2$ (groupe d'inertie sauvage) est impossible puisque $I_v^{wild}$ est distingué dans $I_v$.

### C.1 Calcul de $(-1)^{ord_p(C_v)}$

1. Si $E/K_v$ a réduction potentiellement multiplicative :

   (a) Si $E/K_v$ acquiert réduction multiplicative déployée de type $I_n$ sur $L_z$ (et donc sur $\left(L^{C_p}\right)_w$), alors :

$$\begin{aligned} C_v(\{1\}) = c_w(E/L_z) &= e_{L_z/\left(L^{C_p}\right)_w} \times c_{w'}(E/\left(L^{C_p}\right)_w) \\ &= \frac{e_{\{1\}}}{e_{C_p}} \times c_v(E/K) C_v(C_p) \\ &= \frac{e_{\{1\}}}{e_{C_p}} \times C_v(C_p) \end{aligned}$$

   or si $I_v = C_p$ alors $e_{\{1\}} = p$ et $e_{C_p} = 1$ et si $I_v = D_{2p}$ alors $e_{\{1\}} = 2p$ et $e_{C_p} = 2$. Dans les deux cas, on obtient :

$$C_v = p \text{ et } (-1)^{ord_p(C_v)} = -1.$$

   (b) Si $E/K_v$ n'acquiert pas réduction multiplicative déployée de type $I_n$ sur $L_z$ (et donc pas plus sur $\left(L^{C_p}\right)_w$), alors :

$$c_v(\{1\}), c_v(C_p) \in \{1,2,3,4\} \text{ et } ord_p\left(\frac{\omega(\{1\})}{\omega(C_p)}\right) \equiv 0 \,(\mathrm{mod}\, 2)\,.$$

   La seconde affirmation est une conséquence de la proposition 4.2.7.4 dans le cas $l_v \neq p$.
   Dans le cas $l_v = p$, on doit distinguer deux cas :

   i. Si $E/K_v$ acquiert réduction multiplicative non déployée de type $I_n$ sur $L_z$ (et donc sur $\left(L^{C_p}\right)_w$), alors $\delta_{\{1\}} = \delta_{C_p}$.
   De plus, $f_{C_p} = f_{\{1\}} = 1$ ou $2$ et $\dfrac{\omega(\{1\})}{\omega(C_p)} = q^{\delta f(e_{\{1\}} - e_{C_p})}$, donc

$$ord_p\left(\frac{\omega(\{1\})}{\omega(C_p)}\right) \equiv 0 \,(\mathrm{mod}\, 2) \;\; (\text{car } p-1 \mid \left(e_{\{1\}} - e_{C_p}\right)).$$

   ii. Si $E/K_v, E/\left(L^{C_p}\right)_w$ et $E/L_z$ ont réduction additive (de type $I_n^*$) :
   • Si $I_v = C_p$, alors $f_{C_p} = f_{\{1\}} = 2$ et le résultat en découle.

• Si $I_v = D_{2p}$, puisque $p \geq 5$, $E$ devient de type $I^*_{2n}$ sur $\left(L^{C_p}\right)_w$ et $I^*_{2pn}$ sur $L_z$ et on obtient :

$$ord_p\left(\omega\left(\{1\}\right)\right) = ord_p\left(\omega\left(C_p\right)\right) \equiv 0 \pmod 2.$$

*Pour résumer, dans le cas de la réduction potentiellement multiplicative :*

$$(-1)^{ord_p(C_v)} = \left\{ \begin{pmatrix} -1 & \text{si } E/(L^{C_p}) \text{ a réduction multiplicative déployée} \\ 1 & \text{sinon.} \end{pmatrix} \right.$$

2. Si $E/K_v$ a potentiellement bonne réduction, alors :

   (a) Si $I_v = C_p$ (i.e. $e_{\{1\}} = p$ et $e_{C_p} = 1$) :
   On obtient : $f_{\{1\}} = f_{C_p} = 2$ donc $ord_p(\omega(C_p)) \equiv ord_p(\omega(\{1\})) \equiv 0 \pmod 2$
   et donc $(-1)^{ord_p(C_v)} = 1$ (voir la proposition 4.2.7.2).

   (b) Si $I_v = D_{2p}$ (i.e. $e_{\{1\}} = 2p$, $e_{C_p} = 2$ et $l_v = p$), on obtient :

$$\frac{C_v(\{1\})}{C_v(C_p)} = \frac{\omega(\{1\})}{\omega(C_p)} = q^{\left\lfloor \frac{\delta . e_{\{1\}}}{12} \right\rfloor - \left\lfloor \frac{\delta . e_{C_p}}{12} \right\rfloor} = q^{\lfloor \frac{\delta . 2p}{12} \rfloor - \lfloor \frac{\delta . 2}{12} \rfloor}.$$

   Si $q$ est une puissance paire de $p$, alors

$$(-1)^{ord_p(C_v)} = (-1)^{ord_p\left(\frac{\omega(\{1\})}{\omega(C_p)}\right)} = 1.$$

      i. Si $q$ est une puissance impaire de $p$ :
      Le calcul de $\left\lfloor \frac{\delta.2p}{12} \right\rfloor$ et $\left\lfloor \frac{\delta.2}{12} \right\rfloor$ dépend de $p$ modulo 12 et donne la table suivante :
      Table des valeurs de $(-1)^{ord_p(C_v)}$ en fonction du symbole de Kodaira de la courbe (et de la valeur de $\mathfrak{e} = \frac{12}{\text{pgcd}(\delta,12)}$) et $p \bmod 12$ :

| $p \bmod 12$ | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| $II, II^*$ $(\mathfrak{e} = 6)$ | 1 | -1 | 1 | -1 |
| $III, III^*$ $(\mathfrak{e} = 4)$ | 1 | 1 | -1 | -1 |
| $IV, IV^*$ $(\mathfrak{e} = 3)$ | 1 | -1 | 1 | -1 |
| $I^*_o$ $(\mathfrak{e} = 2)$ | 1 | 1 | 1 | 1 |

      En lien avec le tableau ci-dessus, il peut être utile de rappeler le fait suivant : Si la caractéristique résiduelle de $K_v$ est $> 3$, alors on a la correspondance suivante entre $\mathfrak{e} = \frac{12}{\text{pgcd}(\delta,12)}$, la valuation du discriminant minimal $\delta$ et les symboles de Kodaira :
      $\mathfrak{e} = 1 \quad \Leftrightarrow \delta = 0 \qquad \Leftrightarrow E$ est de type $I_0$
      $\mathfrak{e} = 2 \quad \Leftrightarrow \delta = 6 \qquad \Leftrightarrow E$ est de type $I^*_0$
      $\mathfrak{e} = 3 \quad \Leftrightarrow \delta = 4$ ou $8 \quad \Leftrightarrow E$ est de type $IV$ ou $IV^*$
      $\mathfrak{e} = 4 \quad \Leftrightarrow \delta = 3$ ou $9 \quad \Leftrightarrow E$ est de type $III$ ou $III^*$
      $\mathfrak{e} = 6 \quad \Leftrightarrow \delta = 2$ ou $10 \quad \Leftrightarrow E$ est de type $II$ ou $II^*$.
      Pour la signification des symboles de Kodaira on pourra regarder p.354 de [58].

## C.2 Calcul de $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}$

1. Les cas de la réduction potentiellement multiplicative :
On a une formule explicite de Rohrlich (voir [46] Th.2 (ii) p.329) :
$W(E/K_v,\sigma)=\det\sigma(-1)\chi(-1)^{\dim\sigma}(-1)^{\langle\chi,\sigma\rangle}$,
où $\chi$ est le caractère de $K_v^*$ associé à l'extension $K_v(\sqrt{-c_6})$ de $K_v$ ($c_6$ est la constante classique liée à la courbe $E$, voir par exemple p.46 de [59]).
Comme $\dim\tau_v=\dim 1\oplus\eta=2$, $\det(\tau_v)=\det(1\oplus\eta)$ et $\langle\chi,\tau_v\rangle=0$, on obtient :

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=\frac{(-1)^{\langle\chi,\tau_v\rangle}}{(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}}=\frac{1}{(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}}=(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}.$$

   (a) Si la réduction de $E/K_v$ est multiplicative déployée (i.e. $\chi=1$), alors

$$(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}=-1.$$

   (b) Si la réduction de $E/K_v$ est multiplicative non-déployée (i.e. $\chi$ est un caractère quadratique non-ramifié) :

      i. Si $E$ acquiert réduction multiplicative déployée sur $L_z$ (et donc sur $\left(L^{C_p}\right)_w$), alors $\eta_v=\chi$, et donc $(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}=-1$.
      ii. Si $E$ acquiert réduction multiplicative non-déployée sur $L_z$ (et donc sur $\left(L^{C_p}\right)_w$), alors $\eta_v\neq\chi$, et donc $(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}=1$.

   (c) Si la réduction de $E/K_v$ est additive (i.e. $\chi$ est un caractère quadratique ramifié)

      i. Si $E$ acquiert réduction multiplicative déployée sur $L_z$ (et donc sur $\left(L^{C_p}\right)_w$), alors $\eta_v=\chi$, et donc $(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}=-1$.
      ii. Si $E$ acquiert réduction multiplicative non-déployée sur $L_z$ (et donc sur $\left(L^{C_p}\right)_w$), alors $\eta_v\neq\chi$, et donc $(-1)^{\langle\chi,(1\oplus\eta)_v\rangle}=1$.

*Pour résumer, dans le cas de la réduction potentiellement multiplicative :*

$$\begin{aligned}\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}&=\begin{cases}-1 & \text{si } E/(L^{C_p}) \text{ réduction multiplicative déployée}\\ 1 & \text{sinon.}\end{cases}\\&=(-1)^{ord_p(C_v)}\text{, d'après "Calcul de } (-1)^{ord_p(C_v)}\text{ :.1"}\end{aligned}$$

2. Le cas de la réduction potentiellement bonne :
Ici, on doit distinguer le cas où $l_v=p$ et celui où $l_v\neq p$.

   (a) Le case $l_v=p$.
   On a de nouveau une formule explicite de Rohrlich, car $p\geq 5$ (voir [46], Th.2 (iii) p.329) :
   On utilise les notations suivantes :
   • $q=p^r$ le cardinal du corps résiduel de $K_v$.
   • $\mathfrak{e}=\frac{12}{\text{pgcd}(\delta,12)}$.
   • $\epsilon=\begin{cases}1 & \text{si } r \text{ est pair ou } \mathfrak{e}=1,\\ \left(\frac{-1}{p}\right) & \text{si } r \text{ est impair et } \mathfrak{e}=2 \text{ ou } 6,\\ \left(\frac{-3}{p}\right) & \text{si } r \text{ est impair et } \mathfrak{e}=3,\\ \left(\frac{-2}{p}\right) & \text{si } r \text{ est impair et } \mathfrak{e}=4.\end{cases}$

Alors pour toute représentation auto-duale $\sigma$ de $Gal(\overline{K}_v/K_v)$ d'image finie :

$$W(E/K_v,\sigma)=\begin{cases}\alpha(\sigma,\epsilon) & \text{si } q\equiv 1[\mathfrak{e}]\\ \alpha(\sigma,\epsilon)(-1)^{\langle 1+\eta_{nr}+\hat{\sigma}_e,\sigma\rangle} & \text{si } q\equiv -1[\mathfrak{e}]\\ & \text{et } \mathfrak{e}=3,4,6,\end{cases}$$

où $\eta_{nr}$ est le caractère quadratique non-ramifié, $\hat{\sigma}_e$ est une représentation irréductible de degré 2 de $D_{2\mathfrak{e}}$ et $\alpha(\sigma,\epsilon):=(\det\sigma)(-1)\epsilon^{\dim\sigma}$.
Comme $\dim\tau_v=\dim(1\oplus\eta)_v=2$ et $\det\tau_v=\det(1\oplus\eta)_v$, $\alpha((1\oplus\eta)_v,\epsilon)=\alpha(\tau_v,\epsilon)$ et on obtient :

$$\begin{aligned}\tfrac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} &= \begin{cases}1 & \text{si } q\equiv 1[\mathfrak{e}]\\ (-1)^{\langle 1+\eta_{nr}+\hat{\sigma}_e,1+\eta_v+\tau_v\rangle} & \text{si } q\equiv -1[\mathfrak{e}]\\ & \text{et } \mathfrak{e}=3,4,6,\end{cases}\\ &= \begin{cases}1 & \text{si } q\equiv 1[\mathfrak{e}]\\ (-1)^{\langle 1+\eta_{nr},1+\eta_v\rangle} & \text{si } q\equiv -1[\mathfrak{e}]\\ & \text{et } \mathfrak{e}=3,4,6,\end{cases}\\ &(\langle\hat{\sigma}_e,\tau_v\rangle=0 \text{ comme } \mathfrak{e}=3,4,6 \text{ et } p\geq 5).\end{aligned}$$

i. Si $r$ est pair, alors $q\equiv 1[\mathfrak{e}]$ $\forall\mathfrak{e}\in\{2,3,4,6\}$ et par conséquent

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=1=(-1)^{ord_p(C_v)},$$

d'après 2.b.i (dans la section C.1).

ii. Si $r$ est impair, alors $q\equiv 1[\mathfrak{e}]\iff p\equiv 1[\mathfrak{e}]$ et :

$$\tfrac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=\begin{cases}1 & \text{si } q\equiv 1[\mathfrak{e}]\\ (-1)^{\langle 1+\eta_{nr},1+\eta_v\rangle} & \text{si } q\equiv -1[\mathfrak{e}] \text{ et}\\ & \mathfrak{e}=3,4,6.\end{cases}$$

· Si $I_v=C_p$, alors $\eta_{nr}=\eta_v$ et $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=1$.
· Si $I_v=D_{2p}$, alors $\eta_{nr}\neq\eta_v$ et

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}=\begin{cases}1 & \text{si } q\equiv 1[\mathfrak{e}]\\ -1 & \text{si } q\equiv -1[\mathfrak{e}] \text{ et } \mathfrak{e}=3,4,6.\end{cases}$$

Dans les deux cas, on obtient pour les valeurs de $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}$ exactement la même table que pour les valeurs de $(-1)^{ord_p(C_v)}$, en fonction de $p$ modulo 12 :

Table des valeurs de $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)}$ en fonction du symbole de Kodaira de la courbe (et la valeur de $\mathfrak{e}=\frac{12}{\mathrm{pgcd}(\delta,12)}$) et $p \bmod 12$ :

| $p \bmod 12$ | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| $II, II^*$ $(\mathfrak{e}=6)$ | 1 | -1 | 1 | -1 |
| $III, III^*$ $(\mathfrak{e}=4)$ | 1 | 1 | -1 | -1 |
| $IV, IV^*$ $(\mathfrak{e}=3)$ | 1 | -1 | 1 | -1 |
| $I_o^*$ $(\mathfrak{e}=2)$ | 1 | 1 | 1 | 1 |

(b) Le cas $l_v \neq p$ :
Dans ce cas, la formule explicite de Rohrlich ne peut pas être utilisée car $l_v$ peut valoir 2 ou 3.
Soit $\sigma$ une représentation orthogonale $\sigma : Gal(\overline{K}_v/K_v) \to GL(V_\sigma)$ d'image finie et $\sigma'_{E/K_v} : \mathcal{WD}(\overline{K}_v/K_v) \to GL(V)$ la représentation du groupe de Weil-Deligne, associée à la courbe elliptique, donnée par $\left(\sigma_{E/K_v}, N\right) = \left(\sigma_{E/K_v}, 0\right)$ (car on est dans le cas de potentiellement bonne réduction). C'est simplement une représentation du groupe de Weil $\mathcal{W}(\bar{K}_v/K_v)$ (car $N = 0$) et

$$\sigma'_{E/K_v} \otimes \sigma = \sigma_{E/K_v} \otimes \sigma : \mathcal{W}(\overline{K}_v/K_v) \to GL(W),$$

où $W = V \otimes V_\sigma$, est aussi une représentation du groupe de Weil.
On commence par rappeler la définition des signe locaux (ou "root numbers") via les facteurs epsilon (voir la section 2.4 pour plus de détails) :

$$W(E/K_v, \sigma) = \frac{\varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx)}{\left|\varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx)\right|} = \varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi),$$

où $dx$ est une mesure de Haar, $\psi$ est un caractère additif de $K_v$, $dx_\psi$ est la mesure de Haar auto-duale vis-à-vis de $\psi$ sur $K_v$. Ici, on choisit un caractère additif $\psi$ pour lequel la mesure de Haar $dx_\psi$ est à valeurs (sur les ouverts compactes de $K_v$) dans $\mathbb{Z}_p[\zeta_p]$, où $\zeta_p$ est une racine primitive $p$-ième de l'unité. Par exemple, si le conducteur de $\psi$ est trivial, alors les valeurs de $dx_\psi$ appartiennent à $l_v^{\mathbb{Z}} \cup \{0\} \subset \mathbb{Z}_p[\zeta_p]$. Comme $\sigma$ est une représentation orthogonale, le facteur $\varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi)$ appartient à $\{\pm 1\}$ et est indépendant de $\psi$ (voir par exemple la proposition 2.2.1 de [38]).
Dans l'un de ses articles (voir p.548 de [11]), Deligne donne une description du facteur epsilon $\varepsilon$ en fonction du facteur $\varepsilon_0$. Dans notre cadre, cela donne :

$$\varepsilon(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi) = \varepsilon_0(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi) \det(-(\sigma_{E/K_v} \otimes \sigma)(\Phi) \mid W^{I(v)})^{-1},$$

où $\Phi$ est un Frobenius géométrique en $v$ et $I(v) = Gal(\bar{K}_v/K_v^{ur})$.
Rapellons que, comme $l_v \neq p$, le groupe d'inertie de $D_{2p}$ est $I_v = C_p$.

i. Si $E$ a réduction additive, notons $F$ la plus petite extension galoisienne de $K_v^{ur}$ tel que $E$ acquiert bonne réduction sur $F$ et posons $G_{br} = Gal(F/K_v^{ur})$ alors la restriction de $\sigma_{E/K_v}$ à $I(v)$ se factorise à travers $G_{br}$.
Il est connu que :
• Pour $l_v \geq 5$, $G_{br}$ est cyclique d'ordre $\mathfrak{e} = \frac{12}{\text{pgcd}(\delta,12)}$ (divisant 12).
• Pour $l_v = 3$, $|G_{br}| \in \{2, 3, 4, 6, 12\}$ .
• Pour $l_v = 2$, $|G_{br}| \in \{2, 3, 4, 6, 8, 24\}$ .
Pour une description plus précise de $G_{br}$, on peut regarder [5] ou [29].
La représentation $\sigma_{E/K_v} \otimes \sigma$ (où $\sigma$ est égale à $\tau_v$ ou $(1 \oplus \eta)_v$) restreinte à $I(v)$ se factorise à travers un quotient $H$ de $I(v)$ qui admet $G_{br}$ et $C_p$ comme quotients.
On a :

$$(V \otimes V_\sigma)^{I(v)} = (V \otimes V_\sigma)^H = Hom_H(V^*, V_\sigma) = Hom((V^{G_{br}})^*, V_\sigma^{C_p})$$

car $H$ agit sur $V$ (resp. sur $V_\sigma$) à travers son quotient $G_{br}$ (resp. $C_p$) et $|G_{br}|$ est premier avec $p$.
De plus, $V^H = V^{G_{br}} = \{0\}$ car $E$ a réduction additive, donc

$$(V \otimes V_\sigma)^{I(v)} = 0, \quad \det\left(-\left(\sigma'_{E/K_v} \otimes \sigma \otimes \omega^r\right)(\Phi) \mid (V \otimes V_\sigma)^{I(v)}\right) = 1$$

et

$$(*) \qquad W(E/K_v, \sigma) = \varepsilon_0(\sigma_{E/K_v} \otimes \sigma, \psi, dx_\psi) \quad (\text{où } \sigma \in \{\tau_v, (1 \oplus \eta)_v\}).$$

Deligne donne aussi un résultat de congruence pour les $\varepsilon_0$ (voir la proposition 2.4.18 ou l'article [11] p.556-557). Comme $\chi \equiv 1 \bmod(1-\zeta_p)$, on en déduit que $I(\chi) \equiv I(1) \bmod(1-\zeta_p)$ et que $\sigma'_{E/K_v} \otimes \tau_v \equiv \sigma'_{E/K_v} \otimes (1 \oplus \eta)_v \bmod(1-\zeta_p)$. Donc d'après ce qui précède, $\varepsilon_0(\sigma'_{E/K_v} \otimes \tau_v, \psi, dx_\psi)$ et $\varepsilon_0(\sigma'_{E/K_v} \otimes (1 \oplus \eta)_v, \psi, dx_\psi)$ sont deux éléments de $\{\pm 1\}$ (d'après $(*)$), qui sont congrus modulo $(1-\zeta_p)$, par conséquent ils sont égaux. On en déduit que,

$$\frac{W(E/K_v, \tau_v)}{W(E/K_v, (1 \oplus \eta)_v)} = 1.$$

ii. Si $E$ a bonne réduction, alors $\sigma_{E/K_v}$ est non-ramifié et on a :

$$\varepsilon(\sigma_{E/K_v} \otimes \tau_v, \psi, dx) = \varepsilon(\tau_v, \psi, dx)^{\dim \sigma_{E/K_v}} \det \sigma_{E/K_v}(\varpi_{K_v}^{m(\tau_v,\psi)}),$$

où $m(\tau_v, \psi) \in \mathbb{N}$ dépend des conducteurs de $\tau_v$ et $\psi$, et de la dimension de $\tau_v$ (voir [60] 3.4.6 p.15), par conséquent :

$$W(E/K_v, \tau_v) = W(\sigma_{E/K_v} \otimes \tau_v) = \frac{\varepsilon(\sigma_{E/K_v} \otimes \tau_v, \psi, dx)}{\left|\varepsilon(\sigma_{E/K_v} \otimes \tau_v, \psi, dx)\right|} = 1,$$

car $\det \sigma_{E/K_v} = 1$, $W(\tau_v) = \dfrac{\varepsilon(\tau_v, \psi, dx)}{|\varepsilon(\tau_v, \psi, dx)|} \in \pm 1$ (car $\det \tau_v = 1$, voir la proposition p.145 de [45]) et $\dim \sigma_{E/K_v} = 2$.
De la même façon, $W(E/K_v, (1 \oplus \eta)_v) = 1$, donc $\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = 1$.

Dans les cas i) et ii) on a aussi $(-1)^{ord_p(C_v)} = 1$ d'après 2.a. (dans la section C.1).

Pour résumer, on a, pour toutes places finies $v$ de $K$,

$$\frac{W(E/K_v,\tau_v)}{W(E/K_v,(1\oplus\eta)_v)} = (-1)^{ord_p(C_v)}.$$

Ceci conclut la démonstration du théorème 4.2.2.

**Remarque 4.2.10.** Cette démonstration peut être adaptée pour fonctionner dans le cas où $Gal(L/K) \simeq D_{2p^n}$, les calculs sont presque les mêmes. L'idée de réduire la démonstration au cas d'une $D_{2p}$-extension, grâce au résultat d'invariance de Rohrlich, m'a été suggéré par Tim Dokchitser.

## 4.3 Appendice

Le but de cette appendice est d'apporter une petite amélioration du Théorème 6.7 de [21]. L'intérêt de cette amélioration est que la Proposition 6.12 de [21] (qui dit la même chose que le Théorème 4.1.10 pour $p \equiv 3 \bmod 4$) ne repose plus sur le "truly painful case of additive reduction" (voir p.53 de [18]). En effet, on utilise le passage au cas global pour éviter toutes les places de réduction additive, pas juste les places au-dessus de 2 et 3. Comme on a prouvé le résultat pour $p \geq 5$ (Theorem 4.1.10) sans utiliser de résultats de parité globaux, l'intérêt pour nous est essentiellement le cas où $p = 3$.

On commence par rappeler la définition de la proximité entre deux courbes elliptiques :

**Proposition 4.3.1.** Soit $\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ une courbe elliptique sur un corps local non-archimédien $\mathcal{K}$ (de valuation $v$ et de caractéristique résiduelle $p$) et $\mathcal{F}/\mathcal{K}$ une extension galoisienne finie.
Il existe $\varepsilon > 0$ tel que toutes courbes elliptiques $\mathcal{E}' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ sur $\mathcal{K}$ vérifiant $\forall i \, |a_i' - a_i|_v < \varepsilon$, admettent les propriétés suivantes :
Sur tout corps intermédiaire $\mathcal{F}'$ de $\mathcal{F}/\mathcal{K}$, $\mathcal{E}$ et $\mathcal{E}'$ ont le même :
· conducteur.
· valuation du discriminant minimal.
· facteurs de Tamagawa locaux, $C(E/\mathcal{F}', \frac{dx}{2y+a_1x+a_3})$.
· signes locaux (ou "root numbers").
· module de Tate comme $Gal(\bar{\mathcal{K}}/\mathcal{K})$-module (pour tout $l \neq p$).

On dira que $\mathcal{E}'$ est *proche de* $\mathcal{E}/\mathcal{K}$.

**Démonstration.** C'est la proposition 3.3 de [21]. ■

On énonce maintenant la petite amélioration du théorème 6.7 de [21] :

**Théorème 4.3.2.** Soit $\mathcal{K}$ un corps local non-archimédien de caractéristique 0 et $\mathcal{F}/\mathcal{K}$ une extension galoisienne finie. Soit $F/K$ une extension galoisienne de corps totalement réels et $v_0$ une place de $K$ tel que :
• $v_0$ admet une unique place $\bar{v}_0$ de $F$ au-dessus d'elle
• $K_{v_0} \simeq \mathcal{K}$ et $F_{\bar{v}_0} \simeq \mathcal{F}$.
Une telle extension existe (voir le lemme 3.1 de [21]).
Soit $\mathcal{E}/\mathcal{K}$ une courbe elliptique à réduction additive.
Alors il existe une courbe elliptique $E/K$ tel que :
• $E$ a réduction semi-stable pour tout $w \neq v_0$
• $j(E)$ n'est pas un entier (i.e. $j(E) \notin \mathcal{O}_K$)
• $E/K_{v_0}$ est *proche de* $\mathcal{E}/\mathcal{K}$.

**Démonstration.** On commence par choisir une courbe elliptique $E/K$ tel que $E/K_{v_0}$ est *proche de* $\mathcal{E}/\mathcal{K}$ (c'est possible d'après la proposition 4.3.1).
Maintenant l'objectif est d'enlever toutes les places de réduction additive en changeant $E/K$ en une courbe elliptique vérifiant les trois conditions du théorème.
Soit $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ avec $a_i \in \mathcal{O}_K$.
Si on veut qu'une place $w$ ne soit pas de réduction additive il faut imposer l'une des conditions suivantes :
• La valuation $w(\Delta)$ est nulle (dans ce cas $w$ est de bonne réduction).
• La valuation $w(c_4)$ est nulle (dans ce cas $w$ est de bonne réduction ou de réduction

multiplicative respectivement si $w(\Delta) = 0$ ou $w(\Delta) > 0$).
Soit $v \neq v_0$ une place de $K$ qui n'est pas au-dessus de 2.

Pour obtenir la condiction "$j(E)$ n'est pas un entier " il suffit de faire de $v$ une place de réduction multiplicative ($v$ est une place de réduction multiplicative $\Leftrightarrow v(j(E)) < 0$). On fera ça dans l'étape 2 ci-dessous. Avant de faire ça, on va montrer dans l'étape 1 comment rendre toutes les places au-dessus de 2 semi-stable.
**Etape 1** : **Rendre semi-stable toutes les places** $w \neq v_0$ **au-dessus de** 2
Notons $v_{2,1}, ..., v_{2,r}$ ces places.
Dans ce cas : $\left[v_{2,i}(a_1) = 0 \Rightarrow v_{2,i}(c_4) = 0 \ (c_4 = (a_1^2 + 4a_2)^2 - 24a_1a_3 - 48a_4)\right]$.
Soit $\mathfrak{p}_0$ et $\mathfrak{p}_{2,i}$ les idéaux premiers associés à $v_0$ et $v_{2,i}$.
D'après le théorème des restes chinois, il existe $d_1 \in \mathcal{O}_K$ tel que :
• $d_1 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_1) \geq n$).
• $d_1 \equiv 1 - a_1 \bmod \mathfrak{p}_{2,i}$ $\forall i \in \{1, .., r\}$ (i.e. $v_{2,i}(a_1 + d_1) = 0$).
• $d_1 \equiv -a_1 \bmod \mathfrak{p}$ ($\mathfrak{p}$ associé à $v \neq v_0$).
Donc, si on pose $a_1' = a_1 + d_1$ pour $n$ assez grand on obtient que la courbe $y^2 + a_1'xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ qui est *proche de* $\mathcal{E}/\mathcal{K}$, $v_{2,i}(a_1') = v_{2,i}(a_1 + d_1) = 0$ $\forall i \in \{1, .., r\}$ et $v(a_1') > 0$.
**Etape 2** : **Rendre** $v$ **semi-stable**
D'après le théorème des restes chinois, il existe $d_2, d_3, d_4 \in \mathcal{O}_K$ tel que :
- $d_2 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_2) \geq n$)
  $d_2 \equiv 1 - a_2 \bmod \mathfrak{p}$ (donc $v(a_2 + d_2) = 0$).
- $d_3 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_3) \geq n$)
  $d_3 \equiv -a_3 \bmod \mathfrak{p}$ (so $v(a_3 + d_3) > 0$).
- $d_4 \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(d_4) \geq n$)
  $d_4 \equiv -a_4 \bmod \mathfrak{p}$ (so $v(a_4 + d_4) > 0$).

Donc, si on pose $a_i' = a_i + d_i$, $i \in \{2, 3, 4\}$, pour $n$ assez grand on obtient :
$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6$ est *proche de* $\mathcal{E}/\mathcal{K}$ (Proposition 4.3.1).
De plus : • $c_4' = (a_1'^2 + 4a_2')^2 - 24a_1'a_3' - 48a_4'$
• $v(a_1') > 0$
• $v(a_3') > 0$
• $v(a_4') > 0$
• $v(a_2') = 0$,
donc $v(c_4') = 0$.

La courbe $E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6$ est *proche de* $\mathcal{E}/\mathcal{K}$. De plus, $\forall w \neq v_0$ au-dessus de 2, $w(c_4') > 0$, et $v(c_4') = 0$. Comme $c_4'$ ne dépend pas de $a_6$, on peut modifier $a_6$ pour permettre aux places $w \neq v_0$ tel que $w(c_4') > 0$ de devenir des places de bonne réduction (comme $c_4'$ restera inchangé, certaines places de bonne réduction peuvent devenir multiplicative mais pas additive) et tel que $v$ est une place de réduction multiplicative ($v(j(E)) < 0$). C'est ce qu'on fait dans la dernière étape ci-dessous.

**Etape 3**. **Transformer les places de réduction additive en places de bonne réduction et rendre** $v$ **multiplicative.**
Soit $v_1, ..., v_r, v_{r+1}, ..., v_t$ les places où $v_i(c_4') > 0$, $v_i \neq v_0$ ($\neq v$ et pas au-dessus de 2).
Ci-dessus, les places $v_1, ..., v_r$ sont de bonne réduction et les places $v_{r+1}, ..., v_t$ sont de réduction additive pour la courbe $E'$ construite dans l'étape 2.
Soit $b_2$, $b_4$, $b_6$, $b_8$ et $\Delta$ les quantités suivantes associées à $E'$ :

$b_2 = a_1'^2 + 4a_2'$
$b_4 = 2a_4' + a_1'a_3'$
$b_6 = a_3'^2 + 4a_6$
$b_8 = a_1'^2 a_6 + 4a_2'a_6 - a_1'a_3'a_4' + a_2'a_3'^2 - a_4'^2$
et $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$
$= \alpha + \beta a_6 + 16a_6^2$,
où $\alpha = [-b_2^2(-a_1'a_3'a_4' + a_2'a_3'^2 - a_4'^2) - 8b_4^3 - 27a_3'^4 + 9b_2b_4a_3'^2]$
et $\beta = [-b_2^3 - 216a_3'^2 + 36b_2b_4]$
Soit $\gamma = \beta + 32a_6$ ; on sait que 16 est inversible mod $\mathfrak{p}_i$ $\forall i \in \{1, .., t\}$ (car $\mathfrak{p}_i$ n'est pas au-dessus de 2).

d'après le théorème des restes chinois, il existe $c$ tel que :
• $c \equiv 0 \bmod \mathfrak{p}_0^n$ (i.e. $v_0(c) \geq n$)
• $c \equiv 0 \bmod \mathfrak{p}_i$ $\forall i \in \{1, .., r\}$ (i.e. $v_i(c) > 0$)
• $16c \equiv \alpha_i - \gamma \bmod \mathfrak{p}_i$ $\forall i \in \{r+1, .., t\}$ (où $\alpha_i \neq 0, \gamma \bmod \mathfrak{p}_i$)
(i.e. $\forall i \in \{r+1, .., t\}$ , $v_i(\gamma + 16c) = 0$ et $v_i(c) = 0$)
• $c \equiv -a_6 \bmod \mathfrak{p}$ (i.e. $v(a_6') > 0$).
Finalement, si on pose $a_6' = a_6 + c$, pour $n$ assez grand, o, obtient :
$E'' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$
et on voit que :
· $v_1, ..., v_t$ sont des places de bonne réduction pour $E''$.
· $v$ est une place de réduction multiplicative pour $E''$.
Ce qui conclut la démonstration. ■

# Chapitre 5

# Généralisation d'une formule de Rohrlich

Dans tout ce chapitre $K$ est un corps local, extension finie de $\mathbb{Q}_l$ et $q$ est le cardinal du corps résiduel de $K$.

## 5.1 Représentations irréductibles, modérément ramifiées, du groupe de Weil

### 5.1.1 Représentations irréductibles et modérément ramifiées

Soit $\rho$ une représentation irréductible modérement ramifiée de $\mathcal{W}_K = \mathcal{W}(\overline{K}/K)$ (voir le chapitre 1 pour la définition). Dans ce cas, $\rho$ se factorise à travers $\mathcal{W}_K/G_1(L/K)$ où $G_1$ désigne le groupe d'inertie sauvage et donc $\rho$ se factorise à travers un groupe $G = C_n \rtimes \mathbb{Z}$ (où $C_n = \langle c \rangle$ représente l'inertie modérée donc $\text{pgcd}(q, n) = 1$ et $\mathbb{Z} = \langle \Phi \rangle$ est le groupe engendré par le Frobenius géométrique $\Phi$). On a de plus $c^n = 1$ et $c^i \Phi^j = \Phi^j c^{iq^j}$. Le groupe $G$ agit par conjugaison sur les caractères de $C_n$ : $({}^g\chi)(a) = \chi(g^{-1}ag)$ (en particulier $({}^\Phi\chi)(c) = \chi(c)^q$).

Déterminons les représentations irréductibles de $G = C_n \rtimes \mathbb{Z}$.

Soit $\chi : C_n \longrightarrow \mu_n$, $G_\chi = C_n \rtimes m\mathbb{Z}$ son stabilisateur où $\xi = \chi(c) \in \mu_n$, $O(\xi)$ est l'ordre de $\xi$ et $m = \min_i\{i \geq 1 \,|\, \xi^{q^i} = \xi\} = \min_i\{i \geq 1 \,|\, q^i \equiv 1 \,(\text{mod}(O(\xi))\}$. On étend $\chi$ à $G_\chi$ en $\tilde{\chi}$ par $\tilde{\chi}(c^i \Phi^{mj}) = \xi^i$ ($\tilde{\chi}$ est à valeur dans $\mu_{O(\xi)} \subset \mu_n$).

Pour tout $\varphi \in Hom_{Ab}(\Phi^{m\mathbb{Z}}, \mathbb{C}^*)$, on obtient $\tilde{\chi}\varphi = \tilde{\chi}(\varphi \circ \pi) : G_\chi \longrightarrow \mathbb{C}^*$.

On pose alors $V_{\xi,\alpha} = V_{\chi,\varphi} = Ind_{G_\chi}^G \tilde{\chi}\varphi$. La représentation $V_{\xi,\varphi}$ est irréductible de dimension $n$ et ne dépend que de l'orbite de $\chi = \{{}^\Phi\chi, {}^{\Phi^2}\chi, ..., {}^{\Phi^m}\chi = \chi\}$. On a noté $\xi = \chi(c)$ et $\alpha = \varphi(\Phi^m)$.

Donnons des formules explicites pour $V_{\xi,\alpha}$ :

$$V_{\xi,\alpha}(\Phi) = \begin{pmatrix} 0 & \cdots & 0 & \alpha \\ 1 & & & 0 \\ 0 & & & \\ 0 & \cdots & 0 & 1 \quad 0 \end{pmatrix} \text{ et } V_{\xi,\alpha}(c) = \begin{pmatrix} \xi^q & 0 & \cdots & 0 \\ 0 & \xi^{q^2} & & \\ & & & 0 \\ 0 & \cdots & 0 & \xi^{q^m} \end{pmatrix}$$

où $\xi^{q^m} = \xi$.

### 5.1.2 Représentations irréductibles, modérément ramifiées et auto-duales

Notons tout d'abord que la représentation $\rho = V_{\xi,\alpha}$ est auto-duale si et seulement si il existe une matrice $A \in GL_m(\mathbb{C})$ tel que $\begin{cases} {}^t\rho(\Phi)A\rho(\Phi) = A, \\ {}^t\rho(c)A\rho(c) = A. \end{cases}$

On a immédiatement que ${}^t\rho(c)A\rho(c) = (\xi^{q^i+q^j}A_{i,j})_{1\leq i,j\leq m}$, on en déduit que :

$$ {}^t\rho(c)A\rho(c) = A \Longleftrightarrow (\xi^{q^i+q^j}A_{i,j})_{1\leq i,j\leq m} = (A_{i,j})_{1\leq i,j\leq m}.$$

Ainsi si ${}^t\rho(c)A\rho(c) = A$ et $A_{i,j} \neq 0$ alors $O(\xi) \mid q^i + q^j$. En particulier, si $A_{ii} \neq 0$ alors $O(\xi) \mid 2q^i$ puis $O(\xi) \mid 2$ et $q \equiv 1 \bmod(O(\xi))$ donc $m = 1$. Autrement dit, si $m \geq 2$ alors $A_{ii} = 0$.

De plus, si $i \neq j$ $(i < j)$ et $A_{i,j} \neq 0$ alors $O(\xi) \mid q^i + q^j = q^i(1 + q^{j-i})$ et donc $O(\xi) \mid 1 + q^{j-i}$ et $q^{j-i} \equiv -1 \bmod(O(\xi))$ et par conséquent $2(j-i) = m$. Ainsi $m$ est paire et on a nécessairement $|j-i| = \frac{m}{2}$. On peut donc synthétiser les résultats de la façon suivante :

1. Si $2 \nmid m$ alors $\xi = \pm 1$, $m = 1$ et $\alpha = \pm 1$.
2. Si $2 \mid m$ alors $A = \begin{pmatrix} 0 & C \\ B & 0 \end{pmatrix}$ avec $B$ et $C$ des matrices diagonales de $GL_{\frac{m}{2}}(\mathbb{C})$.

   Comme ${}^t\rho(\Phi)A\rho(\Phi) = A$, on a $B = dI_{\frac{m}{2}}$ et $C = \alpha d I_{\frac{m}{2}}$ avec $\alpha = \pm 1$.

   Réciproquement, $\forall d \in \mathbb{C}^*$, si $\alpha = \pm 1$ alors $A = d\begin{pmatrix} 0 & I_{\frac{m}{2}} \\ \alpha I_{\frac{m}{2}} & 0 \end{pmatrix}$ défini une application bilinéaire non-dégénérée et $G$-invariante de $V_{\xi,\alpha} \times V_{\xi,\alpha} \longrightarrow \mathbb{C}$ qui est symétrique si $\alpha = 1$ et antisymétrique si $\alpha = -1$.

Finalement, on a la proposition suivante :

**Proposition 5.1.1.** Une représentation irréductible, modérément ramifiée et auto-duale de $\mathcal{W}_K$ est de la forme :

$$V_{\xi,1} \text{ ou } V_{\xi,-1}$$

selon qu'elle est orthogonale ou symplectique respectivement.

**Remarque 5.1.2.** La représentation $V_{\xi,1}$ (resp $V_{\xi,-1}$) se factorise à travers le produit semi-direct du groupe cyclique d'ordre $O(\xi)$ (correspondant à l'inertie) par un groupe cyclique d'ordre $m$ (resp $2m$) car $\Phi^m$ (resp $\Phi^{2m}$) agit trivialement sur $V_{\xi,1}$ (resp $V_{\xi,-1}$).

**Proposition 5.1.3.** Soit $K'/K$ une extension finie. On a alors :

$$\dim(V_{\xi,1}^{\mathcal{W}_{K'}}) = \begin{cases} 0 & \text{si } O(\xi) \nmid e, \\ \operatorname{pgcd}(f,m) & \text{si } O(\xi) \mid e, \end{cases}$$

où $e$ et $f$ sont respectivement l'indice de ramification et le degré résiduel de $K'/K$.

**Démonstration.** Cela découle de la description explicite de $V_{\xi,1}$. En effet, si $O(\xi) \nmid e$ alors il n'y a pas d'invariants par le sous-groupe d'inertie de $\mathcal{W}_{K'}$. Par contre, si $O(\xi) \mid e$ alors l'inertie agit trivialement et l'action de $\mathcal{W}_{K'}$ se factorise à travers l'action du groupe cyclique engendré par $\Phi^f$. ∎

### 5.1.3 Lien entre les représentations orthogonales et symplectiques

Si on considère une représentation irréductible auto-duale $V_{\xi,\alpha}$ (donc orthogonale ou symplectique), on peut supposer que $V_{\xi,\alpha}$ est symplectique quitte à tensoriser par un caractère non ramifié.

En effet, soit $ur_\beta : G \longrightarrow \mathbb{C}^*$ tel que $ur_\beta(c) = 1$ et $ur_\beta(\Phi) = \beta$ alors $\rho \otimes ur_\beta(c) = \rho(c)$ et $\rho \otimes ur_\beta(\Phi) = \beta\rho(\Phi)$.

Si on pose $\beta$ tel que $\beta^m = -1$ et $b = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \beta & & \\ \vdots & & & 0 \\ 0 & \cdots & 0 & \beta^{m-1} \end{pmatrix}$ alors :

$$b^{-1}\rho(c)b = \rho(c)$$

et

$$b^{-1}\rho(\Phi)b = \begin{pmatrix} 0 & \cdots & 0 & \alpha\beta^m \\ 1 & & & 0 \\ 0 & & & \vdots \\ 0 & \cdots & 0 & 1 \quad 0 \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 & -\alpha \\ 1 & & & 0 \\ 0 & & & \vdots \\ 0 & \cdots & 0 & 1 \quad 0 \end{pmatrix}.$$

En particulier, $\det V_{\xi,-1} = 1$ et $\det V_{\xi,1} = ur_{-1} = \eta_{ur}$ le caractère non-ramifié d'ordre 2.

On a donc obtenu la proposition suivante :

**Proposition 5.1.4.** Soit $\sigma$ une représentation, symplectique, irréductible et modérement ramifiée du groupe de Weil alors il existe un caractère non-ramifié $ur_\beta$ de $G$ et une représentation orthogonale $\rho$ de $G$ tel que $\sigma = \rho \otimes ur_\beta$.

**Remarque 5.1.5.** Ce résultat nous a été fait remarqué par Guy Henniart.

## 5.2 Classes de Stiefel-Whitney et signe locaux

**Définition 5.2.1.** Un fibré vectoriel $\zeta$ sur $\mathbb{R}$ est un triplet $(E, \pi, B)$ où

1. $E$ (l'espace total) et $B$ (la base) sont des espaces topologiques.
2. $\pi : E \longrightarrow B$ (la projection) est une application continue.
3. $\forall b \in B$, $\pi^{-1}(b)$ est muni d'une structure de $\mathbb{R}$-espace vectoriel qui vérifie :
   $\forall b \in B$, il existe un voisinage ouvert $U$ de $b$, un entier $k$ et un homéomorphisme

   $$\varphi : U \times \mathbb{R}^k \longrightarrow \pi^{-1}(U)$$

   tel que :
   (a) $\forall x \in U$, $(\varphi \circ \pi)(x, v) = x$ pour tout $v \in \mathbb{R}^k$.
   (b) L'application $v \longrightarrow \varphi(x, v)$ est un isomorphisme entre $\mathbb{R}^k$ et $\pi^{-1}(x)$.

**Remarque 5.2.2.** Remarque si on peut choisir $U = B$, le fibré vectoriel est dit trivial.

**Définition 5.2.3** (Classes de Stiefel-Whitney)**.** Pour tout fibré vectoriel réel $\zeta = (E, \pi, B)$, il existe des classes de cohomologie $w_n(\xi) \in H^n(B, \mathbb{Z}/2\mathbb{Z})$, $n \in \mathbb{N}$ vérifiant les axiomes suivants :

1. $w_0(\zeta) = 1$.
2. $w_n(\zeta) = 0$ pour $n$ strictement supérieur à la dimension des fibres.
3. Si $f : B' \longrightarrow B$ est une application continue, alors :
$$f^*(w_n(\zeta)) = w_n(f^*(\zeta)).$$
4. Si $\zeta$ et $\zeta'$ sont deux fibrés vectoriels de base $B$ alors pour tout $k \in \mathbb{N}$ :
$$w_k(\zeta \oplus \zeta') = \sum_{i=1}^{k} w_i(\zeta) \cup w_{k-i}(\zeta')$$
où $\zeta \oplus \zeta'$ désigne la somme de Whitney de $\zeta$ et $\zeta'$.
5. $w_1(\gamma^1) \neq 0$ où $\gamma^1$ désigne le fibré en droite canonique sur $\mathbb{R}P^1$ (l'espace projectif réel de dimension 1).

Donnons quelques propriétés des classes de Siefel-Whitney

**Proposition 5.2.4.** Soit $\zeta$ et $\eta$ deux fibrés vectoriels réels alors :

1. Si $\eta$ est isomorphe à $\zeta$ alors pour tout $i \in \mathbb{N}$, $w_i(\zeta) = w_i(\eta)$.
2. Si $\zeta$ est trivial alors $w_i(\zeta) = 0 \ \forall i > 0$.
3. Si $\eta$ est trivial alors pour tout $i \in \mathbb{N}$, $w_i(\zeta \oplus \eta) = \eta$.

**Définition 5.2.5.** Soit $G$ un groupe fini et $\rho : G \longrightarrow O(V)$ est une représentation orthogonale (i.e réalisable sur $\mathbb{R}$) alors on peut lui associer le fibré vectoriel suivant :

$$\zeta_V : \begin{array}{c} V \times_G E_G \\ \downarrow \\ B_G \end{array} \quad \text{défini par} \quad \begin{array}{ccc} V \times_G E_G & \longrightarrow & E_G \\ & \searrow & \downarrow \\ & & B_G \end{array}$$

où $B_G$ désigne l'espace classifiant de $G$ et $\begin{array}{c} E_G \\ \downarrow \\ B_G \end{array}$ son fibré universel.

**Définition 5.2.6.** On appelle classe de Stiefel-Whitney de $\rho : G \longrightarrow O(V)$ la classe de Stiefel-Whitney de $\zeta_V$, autrement dit $w_*$ est le morphisme composé suivant :

$$R(G, \mathbb{R}) \longrightarrow KO(B_G) \xrightarrow{w_*} H^*(B_G, \mathbb{Z}/2\mathbb{Z})^\times = H^*(G, \mathbb{Z}/2\mathbb{Z})^\times$$

où $R(G, \mathbb{R})$ désigne les représentations de $G$ réalisable sur $\mathbb{R}$ et $KO(B_G)$ le groupe de Grothendieck des fibrés vectoriels sur $B_G$.

**Remarque 5.2.7.**
1. L'isomorphisme $H^1(G, \mathbb{Z}/2\mathbb{Z}) \simeq Hom(G, \{\pm 1\})$, nous permet d'identier $w_1(V)$ au caractère $g \mapsto \det \rho(g)$.
2. Le groupe $H^2(G, \mathbb{Z}/2\mathbb{Z})$ classifie les extensions centrales de $G$ par le groupe à 2 éléments. Si $w_1(V) = 0$ alors $w_2(V)$ est la classe de l'extension image réciproque par $\rho$ du revêtement double $Spin(V, Q)$ de $SO(V, Q)$ où $Q$ est une forme quadratique $G$-invariante définie positive quelconque sur $V$.

**Définition 5.2.8.** Soit $K/\mathbb{Q}_l$ une extension finie, $L/K$ une extension finie galoisienne de groupe $G = Gal(L/K)$ et $\rho : G \longrightarrow O(V)$ est une représentation orthogonale. On identifie $w_1(\rho) = \det \rho$ à un élément $u$ de $K^\times/K^{\times 2}$ par le morphisme injectif suivant :

$$H^1(G, \mathbb{Z}/2\mathbb{Z}) \overset{\text{infl}}{\hookrightarrow} H^1(G_K, \mathbb{Z}/2\mathbb{Z}) \simeq K^\times/K^{\times 2}$$

On notera $Cl$ l'application suivante :

$$Cl : H^2(G, \mathbb{Z}/2\mathbb{Z}) \overset{\text{infl}}{\longrightarrow} H^2(G_K, \mathbb{Z}/2\mathbb{Z}) \overset{\alpha}{\simeq} H^2(G_K, \bar{K}^*)[2] \overset{\text{inv}}{\longrightarrow} (\mathbb{Q}/\mathbb{Z})[2] \overset{x \longmapsto e^{2i\pi x}}{\longrightarrow} \{\pm 1\}$$

où $\alpha$ se déduit de $\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \bar{K}^* \\ n & \to & (-1)^n \end{array}$ et inv est donné par la théorie du corps de classe local (voir par exemple le théorème 2.1 de [34]). On notera souvent encore $w_2(V) = w_2(\zeta_V) \in \{\pm 1\}$ l'image de $w_2(V) = w_2(\zeta_V)$ par $Cl$.

**Théorème 5.2.9.** Si $V$ est une représentation orthogonale de dimension 0 et de déterminant trivial d'un groupe fini $G$ (et $\zeta_V$ le fibré vectoriel sur l'espace classifiant $BG$ de $G$ associé à $V$) alors

$$W(V) = w_2(\zeta_V)$$

où $W(V)$ est le signe local (ou "root number") définit au chapitre 2.

**Démonstration.** C'est le théorème 1.5 de [12]. ■

**Corollaire 5.2.10.** Soit $K$ un corps local, $K'$ une extension galoisienne finie de $K$, $G := Gal(K'/K)$ et $\psi$ est un caractère additif de $K$. Si $V$ est une représentation orthogonale de $G$ alors

$$W(V, \psi) = W(\det V, \psi) w_2(\zeta_V)$$

**Démonstration.** On a que $V = V' \oplus (n-1).1 \oplus \det V$, donc $W(V, \psi) = W(V', \psi) W((n-1).1, \psi) W(\det V, \psi)$ (où $n = \dim V$). Par ailleurs, $W((n-1).1, \psi) = W(1, \psi)^{n-1} = 1$ et $W(V', \psi) = w_2(\zeta_{V'})$ d'après le théorème (car $V'$ est de dimension 0 et de déterminant trivial. De plus $w_2(V') = w_2(V)$. En effet,

$$\begin{aligned} w_2(V) &= w_2(V' \oplus (n-1).1 \oplus \det V) \\ &= w_2(V') + w_1(V') w_1((n-1).1 \oplus \det V)) + w_2((n-1).1 \oplus \det V). \end{aligned}$$

On a $w_2((n-1).1 \oplus \det V) = w_2((n-1).1) + w_1((n-1).1) w_1(\det V) + w_2(\det V)$. Or $w_2((n-1).1) = w_1((n-1).1) = 0$ (car $w_2(1) = w_1(1) = 0$) et $w_2(\det V) = 0$ (car $\det V$ est de dimension 1). Enfin $w_1(\det V') = 0$ (car $\det V'$ est trivial). Finalement, $w_2(V) = w_2(V')$.

■

**Proposition 5.2.11.** Soient $V_1$ et $V_2$ deux représentations orthogonales (de dimension $n$ et $m$ respectivement) de $G$ et $\zeta_V$ et $\zeta_{V'}$ les fibrés vectoriels associés alors

$$\begin{aligned} w_2(\zeta_{V1} \otimes \zeta_{V_2}) = \; & n.w_2(\zeta_{V_1}) + m.w_2(\zeta_{V_2}) + \tfrac{n(n-1)}{2}.w_1(\zeta_{V_1}) \cup w_1(\zeta_{V_1}) \\ & + \tfrac{m(m-1)}{2} w_1(\zeta_{V_2}) \cup w_1(\zeta_{V_2}) + (mn-1) w_1(\zeta_{V_1}) \cup w_1(\zeta_{V_2}). \end{aligned}$$

**Démonstration.** Voir le problème 7C p.87 de [35]. ■

On rappelle que le cup-produit $H^1(G_K, \{\pm 1\}) \times H^1(G_K, \{\pm 1\}) \longrightarrow H^2(G_K, \{\pm 1\})$ s'identifie au symbole de Hilbert $(,-)_2 : K^\times/K^{\times 2} \times K^\times/K^{\times 2} \longrightarrow \{\pm 1\}$ (voir par exemple la section III.4 de [34]).

**Proposition 5.2.12.** Soit $K$ un corps local, $K'$ une extension galoisienne finie de $K$, $G := Gal(K'/K)$ et $\psi$ est un caractère additif de $K$. Soient $V_1$ et $V_2$ deux représentations orthogonales (de dimension $n$ et $m$ respectivement) de $G$, alors $\frac{W(V_1 \otimes V_2, \psi)}{W(\det(V_1 \otimes V_2), \psi)}$ est égal à :

$$\left(\frac{W(V_1,\psi)}{W(\det V_1,\psi)}\right)^m \left(\frac{W(V_2,\psi)}{W(\det V_2,\psi)}\right)^n (u,-1)_2^{\frac{m(m-1)}{2}} (u',-1)_2^{\frac{n(n-1)}{2}} (u,u')_2^{mn-1}$$

où $u$ et $v$ sont des éléments de $K^\times/K^{\times 2}$ qui correspondent respectivement à $w_1(V_1)$ et $w_1(V_2)$ dans l'identification faite dans la définition 5.2.8.

**Démonstration.** C'est simplement la traduction en termes de root numbers de la proposition précédente et du fait que $w_1(\zeta_V) \cup w_1(\zeta_V)$, $w_1(\zeta_W) \cup w_1(\zeta_W)$ et $w_1(\zeta_V) \cup w_1(\zeta_W)$ coincident avec le symbole de Hilbert de $(u,u)_2 = (u,-1)_2$, $(u',u')_2 = (u',-1)_2$ et $(u,u')_2$ respectivement (par l'identification rappelée ci-dessus). ■

## 5.3 Signe local d'une représentation essentiellement symplectique modérément ramifiée du groupe de Weil tensorisée par une représentation auto-duale

Soit $\sigma$ une représentation (complexe) de $\mathcal{W}_K$ modérement ramifiée, essentiellement symplectique de poids $w$ et $\tilde{\sigma} = \sigma \otimes \omega^{w/2}$ est une représentation symplectique. On notera notamment que $\det \tilde{\sigma}$ est trivial et donc que $\frac{\det \sigma}{|\det \sigma|} = 1$.

Si $\sigma$ est irréductible, elle se factorise à travers $G = C_m \rtimes C$ (où $C_m$ est un groupe cyclique d'ordre $m$ représentant l'inertie modérée et $C$ est le groupe cyclique infini engendré par le Frobenius). On considère par ailleurs une représentation complexe auto-duale $\tau$ de $G_K$. L'objectif de cette partie est de donner une formule pour $W(\sigma \otimes \tau) = W(\tilde{\sigma} \otimes \tau)$ qui généralise la formule de Rohrlich (le point 2. du théorème 3.3.2) qui est précisément le cas où $\dim \sigma = 2$.

On rappelle que le signe local n'est pas sensible à la semi-simplification et on peut donc supposer que $\sigma$ et $\tilde{\sigma}$ sont semi-simple.

**Proposition 5.3.1.** Si $\sigma$ est une représentation semi-simple, essentiellement symplectique de poids $w$ de $\mathcal{W}_K$ alors il existe des représentations $\lambda$ et $\theta$ de $\mathcal{W}_K$ tel que

$$\sigma \simeq \left(\lambda \otimes \omega^{-w/2}\right) \oplus \left(\theta \oplus (\theta^* \omega^{-w})\right)$$

ou encore

$$\tilde{\sigma} = \sigma \otimes \omega^{w/2} = \lambda \oplus \left(\theta' \oplus \theta'^*\right))$$

où $\lambda$ est une représentation symplectique de type galoisienne (i.e se factorise à travers un groupe de Galois fini) et $\theta' = \theta \otimes \omega^{w/2}$.

**Démonstration.** Voir la proposition 6 de [47]. ■

Comme la tensorisation par une puissance réelle de $\omega$ ne modifie pas le signe local (voir le corollaire 2.4.20)et que $W(\sigma_1 \oplus \sigma_2) = W(\sigma_1) \oplus W(\sigma_2)$ on en déduit que pour déterminer $W(\sigma \otimes \tau)$ où $\sigma$ est une représentation (complexe) de $\mathcal{W}_K$ modérement ramifiée, essentiellement symplectique de poids $w$, il suffit de le faire dans le cas où $\tilde{\sigma} = \sigma \otimes \omega^{w/2}$ est symplectique et irréductible et dans le cas où $\tilde{\sigma} = \theta \oplus \theta^*$.

### 5.3.1 Le cas où $\tilde{\sigma} = \theta \oplus \theta^*$

**Proposition 5.3.2.** Si $\tilde{\sigma} = \theta \oplus \theta^*$ alors

$$W(\sigma \otimes \tau) = (\det \tau(-1))^{\frac{\dim \sigma}{2}} W(\sigma)^{\dim \tau}$$

**Démonstration.** $\begin{aligned} W(\sigma \otimes \tau) &= W(\tilde{\sigma} \otimes \tau) \\ &= W((\theta \oplus \theta^*) \otimes \tau) \\ &= W((\theta \otimes \tau) \oplus (\theta^* \otimes \tau)) \\ &= W((\theta \otimes \tau) \oplus (\theta \otimes \tau)^*) \text{ (car } \tau \text{ est auto-duale)} \\ &= \det(\theta \otimes \tau)(-1) \\ &= (\det \theta(-1))^{\dim \tau} (\det \tau(-1))^{\dim \theta} \\ &= (\det \tau(-1))^{\frac{\dim \sigma}{2}} W(\sigma)^{\dim \tau} \end{aligned}$ ∎

### 5.3.2 Le cas où $\tilde{\sigma}$ est symplectique et irréductible

On rappelle (voir la proposition 5.1.4) que comme $\tilde{\sigma}$ est symplectique, irréductible et modérement ramifiée, il existe $ur_\beta$ un caractère non-ramifié de $G$ et une représentation $\rho$ orthogonale de $G$ tel que $\tilde{\sigma} = \rho \otimes ur_\beta$ et $(ur_\beta)^{\dim \sigma} = ur_{-1} = \eta_{nr}$. Avec les notations précédentes, on a $\tilde{\sigma} = V_{\xi,-1}$ et $\rho = V_{\xi,1}$.

Soit $\tau$ une réprésentation auto-duale de $G$.

1. Si $\tau = \theta \oplus \theta^*$ alors
$$W(\sigma \otimes \tau) = W(\tilde{\sigma} \otimes \tau) = (\det \tilde{\sigma}(-1))^{\frac{\dim \tau}{2}} W(\tau)^{\dim \tilde{\sigma}} = (\det \tau(-1))^{\frac{\dim \sigma}{2}}.$$
2. Si $\tau$ est symplectique alors $W(\sigma \otimes \tau) = W(\tilde{\sigma} \otimes \tau) = 1$ (voir la proposition 2 de [46]).
3. Si $\tau$ est orthogonale (et irréductible) alors :
   (a) Si $\tau$ est non-ramifiée :
   $$\begin{aligned} W(\sigma \otimes \tau) &= W(\sigma)^{\dim \tau} (\det \tau)(\pi^{a(\sigma)}) \quad \text{(voir la proposition 2.4.19),} \\ &= W(\sigma)^{\dim \tau} \end{aligned}$$
   où la dernière égalité découle du fait que $(V_{\xi,-1})^{I_K} = 0$ et donc $a(\sigma) = \dim \sigma$ est paire.
   (b) Si $\tau$ est sauvagement ramifiée. Dans ce cas, on peut utiliser la formule de Deligne-Henniart (voir la proposition 2.4.21) qui nous dit (comme $\rho$ est modérément ramifiée et $\tau$ est plus ramifiée que $\rho$).qu'il existe $\gamma \in K^\times$ tel que $\varepsilon(\sigma \otimes \tau, \psi, dx) = \varepsilon(\tau, \psi, dx)^{\dim \sigma} (\det \sigma)(\gamma)$ et donc :
   $$\begin{aligned} W(\sigma \otimes \tau) &= W(\tau)^{\dim \sigma} \tfrac{(\det \sigma)(\gamma)}{|(\det \sigma)(\gamma)|} \\ &= W(\tau)^{\dim \sigma} && \text{(car } \sigma \text{ est essentiellement symplectique)} \\ &= \det \tau(-1)^{\frac{\dim \sigma}{2}} && \text{(car } \dim \sigma \text{ est paire et } \tau \text{ est auto-duale)} \end{aligned}$$
   (c) Si $\tau$ est modérément ramifiée. On pose $\tilde{\sigma} = \rho \otimes ur_\beta$ (avec $\rho$ orthogonale et $ur_\beta$ est non-ramifié d'ordre $2 \dim \sigma$). On pose $n_\rho = \dim \rho = \dim \sigma$, $n_\tau = \dim \tau$, $\det \rho = u_\rho K^{*2}$, $\det \tau = u_\tau K^{*2}$ (avec l'identification de la définition 5.2.8) et $\psi$ un caractère additif tel que $n(\psi) = 0$ on a :
   $$\begin{aligned} W(\sigma \otimes \tau) &= W(\tilde{\sigma} \otimes \tau) \\ &= W(\tilde{\sigma} \otimes \tau, \psi) \\ &= W(\rho \otimes \tau \otimes ur_\beta, \psi) \end{aligned}$$

puis

$$W(\sigma\otimes\tau) \quad = W(\rho\otimes\tau,\psi)ur_\beta(\pi^{a(\rho\otimes\tau)})$$

car $\dim ur_\beta = 1$, $ur_\beta$ est non ramifié (voir la proposition 2.4.19) et $n(\psi)=0$. Ci-dessous, on note $W(\rho)$ pour $W(\rho,\psi)$ (où $\psi$ est le caractère additif tel que $n(\psi)=0$ choisi ci-dessus) et de même pour $W(\tau)$, $W(\rho\otimes\tau)$, $W(\det\rho)$, $W(\det\tau)$ et $W(\det(\rho\otimes\tau))$ .
Commençons par montrer que :

$$ur_\beta(\pi^{a(\rho\otimes\tau)}) = \begin{cases} 1 & \text{si } 2 \mid n_\tau \text{ et } \tau\neq\rho, \\ -1 & \text{si } n_\tau = 1 \text{ ou } \tau=\rho. \end{cases}$$

On a tout d'abord $a(\rho\otimes\tau) = \mathrm{codim}(\rho\otimes\tau)^I = \dim(\rho\otimes\tau) - \dim(\rho\otimes\tau)^I$. De plus, $\rho$ et $\tau$ sont des représentations irréductibles et orthogonales (représentations dont on a donné une description précise en 5.1). Si $\rho = V_{\xi,1}$ et $\tau = V_{\xi',1}$ alors les coefficients diagonaux de $(\rho\otimes\tau)(c)$ sont de la forme $\xi^{q^i}\xi'^{q^j}$ qui est différent de 1 sauf dans le cas où $\xi=\xi'$ et $q^{\frac{n_\rho}{2}}+1$ divise $q^i+q^j$ ce qui arrive lorsque $|j-i| = \frac{n_\rho}{2}$ c'est à dire précisément $n_\rho$ fois. Par conséquent $\dim(\rho\otimes\tau)^I = \begin{cases} 0 & \text{si } \tau\neq\rho, \\ n_\rho & \text{si } \tau=\rho, \end{cases}$
et donc

$$a(\rho\otimes\tau) = \begin{cases} n_\rho n_\tau & \text{si } \tau\neq\rho, \\ n_\rho(n_\rho-1) & \text{si } \tau=\rho. \end{cases}$$

Enfin, $ur_\beta(\pi^{2n_\rho}) = 1$ et $ur_\beta(\pi^{n_\rho}) = -1$ (car $ur_\beta$ est d'ordre $2n_\rho$) et finalement on en déduit que

$$ur_\beta(\pi^{a(\rho\otimes\tau)}) = \begin{cases} 1 & \text{si } 2 \mid n_\tau \text{ et } \tau\neq\rho, \\ -1 & \text{si } n_\tau = 1 \text{ ou } \tau=\rho. \end{cases}$$

Montrons maintenant que :

$$W(\rho\otimes\tau) = (\det\tau(-1))^{\frac{n_\rho}{2}} W(\rho)^{n_\tau}(u_\rho,u_\tau),$$

où on note $(,)$ pour le symbole de Hilbert $(,)_2$. D'après la proposition 5.2.12, on a que $W(\rho\otimes\tau)$ est égale à :

$$W(\det(\rho\otimes\tau)) \left(\frac{W(\rho)}{W(\det\rho)}\right)^{n_\tau} \left(\frac{W(\tau)}{W(\det\tau)}\right)^{n_\rho} (u_\rho,-1)^{\alpha_\tau}(u_\tau,-1)^{\alpha_\rho}(u_\rho,u_\tau)$$

où $\alpha_\tau = \frac{n_\tau(n_\tau-1)}{2}$ et $\alpha_\rho = \frac{n_\rho(n_\rho-1)}{2}$.

On a par ailleurs les égalités suivantes :
• $W(\det\rho) = W(\eta_{nr}) = 1$.
• $W(\det(\rho\otimes\tau)) = W((\det\rho)^{n_\tau}(\det\tau)^{n_\rho}) = W((\det\rho)^{n_\tau}) = W(\eta_{nr}^{n_\tau}) = 1$.
• $(u_\rho,-1) = \det\rho(-1) = \eta_{nr}(-1) = 1$.
• $n_\rho$ est pair et $\frac{W(\tau)}{W(\det\tau)} \in \{\pm 1\}$ donc $\left(\frac{W(\tau)}{W(\det\tau)}\right)^{n_\rho} = 1$.
• $(u_\tau,-1)^{\frac{n_\rho(n_\rho-1)}{2}} = (\det\tau(-1))^{\frac{n_\rho(n_\rho-1)}{2}} = (\det\tau(-1))^{\frac{n_\rho}{2}}$ (car $n_\rho$ est pair).
On en déduit que :

$$W(\rho\otimes\tau) = (\det\tau(-1))^{\frac{n_\rho}{2}} W(\rho)^{n_\tau}(u_\rho,u_\tau).$$

Déterminons $W(\rho\otimes\tau)$ :
• Si $2 \mid n_\tau$ alors $W(\rho)^{n_\tau}=1$ et $\det\tau=\eta_{nr}$ (d'après la description des représentations orthogonales faites en 5.1). On a (grâce aux propriétés du symbole de Hilbert, voir la proposition 1.2.10) alors $(u_\rho,u_\rho)=(u_\rho,-1)=\eta_{nr}(-1)=1$ et donc $W(\rho\otimes\tau)=(\det\tau(-1))^{\frac{n_\rho}{2}}$.
• Si $n_\tau=1$ alors $(u_\rho,u_\tau)=\eta_{nr}(u_\tau)=(-1)^{v_K(u_\tau)}$ et donc

$$W(\rho\otimes\tau)=(\det\tau(-1))^{\frac{n_\rho}{2}}W(\rho)(-1)^{v_K(u_\tau)}.$$

Finalement,

$$\begin{aligned}
W(\sigma\otimes\tau) &= W(\rho\otimes\tau)ur_\beta(\pi^{a(\rho\otimes\tau)})\\
&= (\det\tau(-1))^{\frac{n_\rho}{2}}\begin{cases} -1 & \text{si } \rho=\tau,\\ -W(\rho)(-1)^{v_K(u_\tau)} & \text{si } \dim\tau=1,\\ 1 & \text{sinon.}\end{cases}\\
&= (\det\tau(-1))^{\frac{n_\rho}{2}}\begin{cases} -1 & \text{si } \rho=\tau,\\ -W(\rho)(-1)^{v_K(u_\tau)} & \text{si } \tau=1 \text{ ou } \tau=\eta_{K(\sqrt{u_\tau})/K},\\ 1 & \text{sinon.}\end{cases}
\end{aligned}$$

où $\eta_{K(\sqrt{u_\tau})/K}$ désigne un caractère quadratique modérément ramifié ou le caractère non-ramifié (qu'on note aussi $\eta_{nr}$).

Enfin, en remarquant que $W(\sigma)=W(\rho\otimes ur_\beta)=W(\rho)ur_\beta(\pi^{a(\rho)})=-W(\rho)$, on peut synthésiser le point 3. ci-dessus dans le théoreme suivant :

**Théorème 5.3.3.** Si $\sigma$ est une représentation essentiellement symplectique irréductible modérément ramifiée de $\mathcal{W}_K$ alors pour toute représentation auto-duale et irréductible $\tau$, on a :

$$W(\sigma\otimes\tau)=(\det\tau(-1))^{\frac{n_\rho}{2}}\begin{cases} -1 & \text{si } \rho=\tau\\ W(\sigma)(-1)^{v_K(u_\tau)} & \text{si } \tau=1 \text{ ou } \tau=\eta_{K(\sqrt{u_\tau})/K}\\ 1 & \text{sinon}\end{cases}$$

On déduit de ce théorème (et des points 1. et 2.), le corollaire suivant :

**Corollaire 5.3.4.** Si $\sigma$ est une représentation essentiellement symplectique irréductible modérément ramifiée de $\mathcal{W}_K$ alors pour toute représentation auto-duale $\tau$, on a :

$$W(\sigma\otimes\tau)=(\det\tau(-1))^{\frac{\dim\sigma}{2}}(-1)^{\langle\mathcal{V},\tau\rangle}$$

où $\cdot\ \mathcal{V}=\rho\oplus\begin{cases}\bigoplus\limits_{\eta\in X_{nr}}\eta & \text{si } W(\sigma)=-1,\\ \bigoplus\limits_{\eta\in X_{mr}}\eta & \text{si } W(\sigma)=1.\end{cases}$
$\cdot\ X_{nr}=\{\eta:\mathcal{W}_K\longrightarrow\{\pm1\} \text{ non ramifié}\}.$
$\cdot\ X_{mr}=\{\eta:\mathcal{W}_K\longrightarrow\{\pm1\} \text{ totalement modérement ramifié}\}.$

**Démonstration.** En effet, si $\tau=\bigoplus\limits_i\tau_i$ avec $\tau_i$ irréductible auto-duale ou de la forme $\theta\oplus\theta^*$ alors $W(\sigma\otimes\tau)=\prod\limits_i W(\sigma\otimes\tau_i)$. Comme le membre de droite de l'égalité du théorème est multiplicative en $\tau$, il suffit de vérifier l'égalité pour $\tau$ irréductible auto-duale ou de la forme $\theta\oplus\theta^*$.
Si $\tau=\theta\oplus\theta^*$ (resp. $\tau$ est symplectique) alors $\langle\mathcal{V},\tau\rangle=0$ et l'égalité se déduit du 1. (resp

2.) ci-dessus.

Si $2 \mid n_\tau$ alors $\langle \mathcal{V}, \tau \rangle = \begin{cases} 1 & \text{si } \tau = \rho \\ 0 & \text{si } \tau \neq \rho \end{cases}$ et $W(\sigma \otimes \tau) = \begin{cases} -(\det \tau(-1))^{\frac{n_\rho}{2}} & \text{si } \tau = \rho \\ (\det \tau(-1))^{\frac{n_\rho}{2}} & \text{si } \tau \neq \rho \end{cases}$

Si $\tau = 1 \in X_{nr}$ (resp. $\tau = \eta_{K(\sqrt{u_\tau})/K} \in X_{mr}$) alors $v_K(u_\tau) \equiv 0 \bmod 2$ (resp. $v_K(u_\tau) \equiv 1 \bmod 2$) et le théorème ci-dessus permet de conclure. ■

**Corollaire 5.3.5.** Si $\sigma$ est une représentation essentiellement symplectique irréductible modérément ramifiée de $\mathcal{W}_K$ alors pour toute représentation auto-duale $\tau$, on a :

$$W(\sigma \otimes \tau) = (\det \tau(-1))^{\frac{\dim \sigma}{2}} (-W(\sigma))^{\dim \tau} (-1)^{\langle 1 \oplus \eta_{nr} \oplus \rho, \tau \rangle}$$

**Démonstration.** On distingue le cas où $l \neq 2$ et le cas où $l = 2$.

1. Le cas où $l \neq 2$. On commencera par remarquer qu'il n'existe pas de représentation irréductible, auto-duale, non triviale, sauvagement ramifiée et de dimension impaire. En effet, le groupe d'inertie sauvage est un groupe d'ordre impair et un groupe fini d'ordre impair n'a aucune représentation irréductible auto-duale non-triviale. Il suffit ensuite de vérifier que dans les autres cas on a bien :

$$(-1)^{\langle \mathcal{V}, \tau \rangle} = (-W(\sigma))^{\dim \tau} (-1)^{\langle 1 \oplus \eta_{nr} \oplus \rho, \tau \rangle}.$$

2. Le cas où $l = 2$. Dans ce cas, il suffit de montrer qu'on a $W(\sigma) = -1$ pour toute représentation symplectique irréductible modérément ramifiée $\sigma$. Une telle représentation est de la forme (d'après la première section du chapitre 5) :

$$\sigma = Ind_{M/K}(\chi\varphi) = Ind_{F/K}(Ind_{M/F}(\chi\varphi))$$

où $M/F$ est l'extension quadratique correspondant aux groupes $C_n \rtimes m\mathbb{Z}$ et $C_n \rtimes 2m\mathbb{Z}$, $\varphi$ est le caractère non ramifié de $M$ et $Ind_{M/F}(\chi)$ est orthogonale irréductible. D'après le théorème de Frölich-Queyrut (voir le théorème 3 de [24]), on a $W(\sigma) = -W(\chi) = -\chi(u)$, où $M = F(u)$ et $u^2 \in 1 + \mathfrak{p}_F$ (car $M/F$ est non-ramifié). De plus, le groupe multiplicatif du corps résiduel de $M$ est d'ordre impair (car $l = 2$) donc $u \in 1 + \mathfrak{p}_M$. Or $\chi$ est modéré donc $\chi(u) = 1$ et $W(\sigma) = -1$.

■

**Remarque 5.3.6.**
1. Je tiens ici à remercier David Rohrlich pour m'avoir indiqué comme résoudre le cas $l = 2$.
2. Dans le cas où $\dim \sigma = 2$, on retrouve le théorème 3.3.1 (dû à Rohrlich).

### 5.3.3 Le cas général d'une représentation symplectique modérement ramifiée

On a vu (proposition 5.3.1) que si $\sigma$ est une représentation, modérément ramifiée, essentiellement symplectique de poids $w$ de $\mathcal{W}_K$ et $\tilde{\sigma} = \sigma \otimes \omega^{w/2}$ alors on peut écrire :

$$\tilde{\sigma}^{ss} = (\theta \oplus \theta^*) \oplus \bigoplus_{i=1}^{r} \tilde{\sigma}_i$$

où $\theta$ est une représentation (pas nécéssairement irréductible) et les $\tilde{\sigma}_i$ sont irréductibles et symplectiques (et se factorisent à travers des groupes finis $G_i$). On a alors le théorème suivant :

**Théorème 5.3.7.** Soit $\sigma$ une représentation de $\mathcal{W}_K$ comme ci-dessus et $\tau$ une représentation (complexe) auto-duale de $G_K$ alors :

$$W(\sigma\otimes\tau)=W(\tilde{\sigma}^{ss}\otimes\tau)=(\det\tau(-1))^{\frac{\dim\tilde{\sigma}}{2}}(\det\theta(-1))^{\dim\tau}(-1)^{\langle\mathcal{V},\tau\rangle}$$

où $\mathcal{V}=\bigoplus_{i=1}^{r}\mathcal{V}_i$ où $\mathcal{V}_i=\rho_i\oplus\begin{cases}\bigoplus_{\eta\in X_{nr}}\eta & \text{si } W(\tilde{\sigma}_i)=-1\\ \bigoplus_{\eta\in X_{mr}}\eta & \text{si } W(\tilde{\sigma}_i)=1\end{cases}$ et $\tilde{\sigma}_i=\rho_i\otimes ur_{\beta_i}$ (avec $ur_{\beta_i}$ un caractère non-ramifié de $G_i$ et $\rho_i$ une représentation orthogonale de $G_i$).

**Remarque 5.3.8.** Si de plus, $\tau$ est une représentation de dimension paire et de déterminant trivial alors :

$$W(\tilde{\sigma}\otimes\tau)=(-1)^{\langle\mathcal{V},\tau\rangle}.$$

C'est le cas notamment des représentations appartenant à $T_{\Theta,p}$ défini au chapitre 3.

**Corollaire 5.3.9.** Soit $\sigma$ une représentation de $\mathcal{W}_K$ comme ci-dessus et $\tau$ une représentation (complexe) auto-duale de $G_K$ alors :

$$W(\sigma\otimes\tau)=(\det\tau(-1))^{\frac{\dim\sigma}{2}}\prod_{i=1}^{r}(-W(\sigma_i))^{\dim\tau}(-1)^{\left\langle\bigoplus_{i=1}^{r}(1\oplus\eta_{nr}\oplus\rho_i),\tau\right\rangle}$$

Dans le cas, d'une courbe elliptique sur un corps $K$ ($[K:\mathbb{Q}_l]<+\infty$ et $l\neq 2,3$) qui a potentiellement bonne réduction, alors la représentation $\sigma'_{E/K}$ du groupe de Weil-Deligne se factorise à travers le groupe de Weil en une représentation $\sigma_{E/K}$ modérement ramifiée (car $l\neq 2,3$) et donc $\tilde{\sigma}_{E/K}$ est symplectique et irréductible de degré 2 ou de la forme $\theta\oplus\theta^*$ (où $\theta$ est caractère). On obtient le corollaire suivant :

**Corollaire 5.3.10.** Si $E/K$ est une courbe elliptique ($[K:\mathbb{Q}_l]<+\infty$ et $l\neq 2,3$) et

$$W(\sigma_{E/K}\otimes\tau)=\begin{cases}(\det\tau(-1))(-W(E/K))^{\dim\tau}(-1)^{\langle 1\oplus\eta_{nr}\oplus\rho,\tau\rangle} & \text{si } \tilde{\sigma}_{E/K} \text{ est sympl et irréd,}\\ (\det\tau(-1))W(E/K)^{\dim\tau} & \text{si } \tilde{\sigma}=\theta\oplus\theta^*.\end{cases}$$

**Remarque 5.3.11.** Le corollaire précédent est précisément la formule de Rohrlich (voir le 2. du théorème 3.3.2).

# Chapitre 6

# Compatibilité entre signes locaux et nombres de Tamagawa

L'objectif de ce chapitre est de démontrer une généralisation de la compatibilité entre les signes locaux et les nombres de Tamagawa qui est le résultat clef de l'article "Regulator constants and the parity conjecture" (voir l'article [18]) qu'on a rappelé au chapitre 3 (voir le théorème 3.4.26 et ses corollaires). Il est à noter qu'on est seulement capable de gérer les cas où $v \nmid p$ (le cas où $v \mid p$ avec $p \neq 2, 3$ est traité pour les courbes elliptiques dans [18], pour nous il reste pour le moment hors d'atteinte). Cette restriction apporte des simplifications notables, on remarquera notamment que notre $C_v(\Theta)$ est simplement le produit des nombres de Tamagwa (pour traiter le cas $v \mid p$, il faudrait introduire une puissance de $p = l_v$ qui généralise le $\omega$ du chapitre 4 et de [18]).

## 6.1 Nombres de Tamagawa

Soient $K$ et $E$ des corps de nombres, $\sigma_{\mathfrak{p}} : G_K \longrightarrow GL(V) \simeq GL_n(E_{\mathfrak{p}})$ une représentation $\mathfrak{p}$-adique, $\sigma_{\mathfrak{p},v} : G_{K_v} \longrightarrow GL_n(E_{\mathfrak{p}})$ sa restriction à $K_v$ et $T$ un $\mathcal{O}_{E_{\mathfrak{p}}}$-sous-réseau stable de $V$.

**Définition 6.1.1** (Nombres de Tamagawa)**.**

1. Si $v$ est une place archimédienne, on pose $Tam(\sigma_{\mathfrak{p},v}) = \#H^1(K_v, T)$.
2. Si $v$ est une place finie telle que $v \nmid p$ (i.e $l_v \neq p$), on note

$$L_f(K_v, V) = \det_{E_{\mathfrak{p}}} H^0(K_v, V) \otimes \left(\det_{E_{\mathfrak{p}}} H^1_f(K_v, V)\right)^{-1}$$

c'est un $E_{\mathfrak{p}}$-espace vectoriel de dimension 1. On a alors

$$\iota_V : L_f(K_v, V) \simeq E_{\mathfrak{p}}$$

où $\iota_V$ provient de la suite exacte suivante :

$$0 \to H^0(K_v, V) \to V_{l_v} \xrightarrow{Fr_v - 1} V_{l_v} \to H^1_f(K_v, V) \to 0.$$

De même, on note

$$L_f(K_v, T) = \det_{\mathcal{O}_{E_{\mathfrak{p}}}} H^0(K_v, T) \otimes \left(\det_{\mathcal{O}_{E_{\mathfrak{p}}}} H^1_f(K_v, T)\right)^{-1}$$

où $H^1_f(K_v,T)$ est l'image réciproque de $H^1_f(K_v,V)$ dans $H^1(K_v,T)$. C'est un $\mathcal{O}_{E_\mathfrak{p}}$-module libre de rang 1 et il existe un isomorphisme canonique entre $L_f(K_v,T)\otimes_{\mathcal{O}_{E_\mathfrak{p}}} E_\mathfrak{p}$ et $L_f(K_v,V)$. On définit alors $Tam(\sigma_{\mathfrak{p},v})$ comme l'unique puissance de $\varpi_{E_\mathfrak{p}}$ (une uniformisante de $\mathcal{O}_{E_\mathfrak{p}}$) telle que :

$$\iota_V(L_f(K_v,T)) = Tam(\sigma_{\mathfrak{p},v})\mathcal{O}_{E_\mathfrak{p}}$$

**Remarque 6.1.2.**
1. Si $E=\mathbb{Q}$ et $\mathfrak{p}=p$ est un nombre premier alors $Tam(\sigma_{\mathfrak{p},v})$ est une puissance de $p$.
2. Il est important de noter que, même si la notation ne le montre pas explicitement, $Tam(\sigma_{\mathfrak{p},v})$ dépend du choix du réseau $T$. Dans les cas que nous considérerons ensuite $Tam(\sigma_{\mathfrak{p},v})$ sera indépendant de $T$ et vaudra même 1.

**Proposition 6.1.3.** On a la formule suivante pour $Tam(\sigma_{\mathfrak{p},v})$ (avec $v$ finie et $l_v\neq p$) :

$$Tam(\sigma_{\mathfrak{p},v}) = \varpi_{E_\mathfrak{p}}^{l_\mathfrak{p}\left((H^1(I_{K_v},T)^{G_{K_v}})_{tors}\right)}.$$

En particulier si $E=\mathbb{Q}$ et $\mathfrak{p}=p$ alors $Tam(\sigma_{p,v}) = \#(H^1(I_{K_v},T)^{G_{K_v}})_{tors}$.

**Démonstration.** Voir la proposition 4.2.2 de [23]. ■

**Proposition 6.1.4.** Si $V^{I_{K_v}}=\{0\}$ alors $(V/T)^{I_{K_v}}$ est fini et

$$Tam(\sigma_{\mathfrak{p},v}) = \varpi_{E_\mathfrak{p}}^{\alpha}$$

où $\alpha = l_\mathfrak{p}\left((V/T)^{G_{K_v}}\right)$.

**Démonstration.** On a la suite exacte suivante :

$$0\longrightarrow T\longrightarrow V\longrightarrow V/T\longrightarrow 0$$

qui donne lieu à la suite exacte :

$$0\longrightarrow T^{I_{K_v}}\longrightarrow V^{I_{K_v}}\longrightarrow (V/T)^{I_{K_v}}\longrightarrow H^1(I_{K_v},T)\longrightarrow H^1(I_{K_v},V).$$

Or $V^{I_{K_v}}=\{0\}$, $(V/T)^{I_{K_v}}$ est de torsion et $H^1(I_{K_v},V)$ est sans torsion donc $(V/T)^{I_{K_v}}\simeq H^1(I_{K_v},T)_{tors}$. On en déduit que $(V/T)^{I_{K_v}}$ est fini et $(V/T)^{G_{K_v}}\simeq (H^1(I_{K_v},T)^{G_{K_v}})_{tors}$ ce qui donne le résultat. ■

**Proposition 6.1.5.** Si $l_v\neq p$ et $\sigma_{p,v}:=\sigma_{A/K_v}: G_{K_v}\longrightarrow GL(V_p)\simeq GL_{2d}(\mathbb{Q}_p)$ est la représentation $p$-adique de $G_{K_v}$ associée à la variété abélienne $A$ (de dimension $d$) alors :

$$Tam(\sigma_{p,v}) = \left(A(K_v)/A_0(K_v)\right)_p$$

où $A_0(K_v)$ désigne l'ensemble des points de $A(K_v)$ de réduction non-singulière et $(*)_p$ signifie la partie $p$-primaire de $*$. C'est une puissance de $p$.

**Démonstration.** Pour $l_v\neq p$, on a :

$$\left(A(K_v)/A_0(K_v)\right)[p^n] \simeq A(K_v)[p^n]/A_0(K_v)[p^n] \simeq \left(A(K_v^{nr})[p^n]/A_0(K_v^{nr})[p^n]\right)^{G_{K_v}}$$

où $K_v^{nr}$ est l'extension maximale non ramifiée de $K_v$. Par ailleurs,

$$A_0(K_v^{nr})[p^n]\simeq T_p(A)^{I_{K_v}}\otimes_{\mathbb{Z}_p}\mathbb{Z}_p/p^n\mathbb{Z}_p et A(K_v^{nr})[p^n]\simeq \left(T_p(A)\otimes_{\mathbb{Z}_p}\mathbb{Z}_p/p^n\mathbb{Z}_p\right)^{I_{K_v}}$$

et donc par passage à la limite inductive :

$$(A(K_v^{nr})/A_0(K_v^{nr}))_p \simeq (T \otimes \mathbb{D}_p)^I/T^I \otimes \mathbb{D}_p$$

où $T = T_p(A)$, $\mathbb{D}_p = \mathbb{Q}_p/\mathbb{Z}_p$ et $I = I_{K_v}$.
Alors à partir de la suite exacte

$$0 \longrightarrow T \longrightarrow T \otimes \mathbb{Q}_p \longrightarrow T \otimes \mathbb{D}_p \longrightarrow 0$$

on obtient

$$0 \longrightarrow T^I \longrightarrow (T \otimes \mathbb{Q}_p)^I \xrightarrow{j} (T \otimes \mathbb{D}_p)^I \longrightarrow H^1(I,T) \longrightarrow H^1(I, T \otimes \mathbb{Q}_p).$$

Du fait que $\left(T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right)^I \simeq T^I \otimes_{\mathbb{Z}} \mathbb{Q}$ et $H^1(I, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \simeq H^1(I,T) \otimes_{\mathbb{Z}} \mathbb{Q}$, on a alors que :

$$0 \longrightarrow (T \otimes \mathbb{D}_p)^I/T^I \otimes \mathbb{D}_p \longrightarrow H^1(I,T) \longrightarrow H^1(I,T) \otimes_{\mathbb{Z}} \mathbb{Q}$$

et donc, comme $H^1(I,T) \otimes_{\mathbb{Z}} \mathbb{Q}$ est sans torsion, que :

$$(T \otimes \mathbb{D}_p)^I/T^I \otimes \mathbb{D}_p \simeq H^1(I,T)_{tors}$$

et finalement :

$$(A(K_v)/A_0(K_v))_p \simeq (H^1(I,T)^{G_{K_v}})_{tors}$$

■

## 6.2 Nombres de Tamagawa et signes locaux

Soit $E$ un corps de nombres et $E_{\mathfrak{p}}$ le complété de $E$ en $\mathfrak{p}$ ($\mathfrak{p} \mid p$ et $p \neq 2$) On note $\mathcal{O}_{E_{\mathfrak{p}}}$ son anneau des entiers et $q = N(\mathfrak{p})$ le cardinal de son corps résiduel. On commence par rappeler les théorèmes suivants :

**Théorème 6.2.1.** Soit $G$ un sous-groupe fini de $GL_n(\mathcal{O}_{E_{\mathfrak{p}}})$ (avec $p \neq 2$) alors l'ordre de $G$ divise

$$\begin{aligned} A_{n,\mathfrak{p}} &= (q^n - q^{n-1})(q^n - q^{n-2})...(q^n - 1) \\ &= q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1). \end{aligned}$$

On a un théorème similaire dans le cas du groupe symplectique (qui nous intéresse car nous considérerons par la suite des représentations essentiellement simplectiques)

**Théorème 6.2.2.** Soit $G$ un sous-groupe fini de $GSp_n(\mathcal{O}_{E_{\mathfrak{p}}})$ (où $n = 2m$ et $p \neq 2$) alors l'ordre de $G$ divise

$$S_{n,\mathfrak{p}}(E) = q^{m^2+1} \prod_{i=1}^{m} (q^{2i} - 1).$$

**Démonstration.** Voir [1] Chap III p.147. ■

### 6.2.1 Détermination des "mauvais" nombres premiers

Soit un prémotif essentiellement symplectique $M = \{(\sigma_{\mathfrak{p}}, V_{\mathfrak{p}})\}_{\mathfrak{p}}$ sur $K$ (voir la définition 1.4.6 et les définitions 2.1.3 et 3.2.4).

Soit $v$ une place de $K$ (et $\iota$ un plongement de $E$ dans $\mathbb{C}$), on considère les représentations $\sigma_{v,\mathfrak{p}} = \sigma_{\mathfrak{p}|G_{K_v}} : G_{K_v} \longrightarrow GL_n(E_{\mathfrak{p}})$ (pour $\mathfrak{p} \nmid l_v$) qui donnent toutes naissance à la même représentation $\sigma_{\iota M,v} : \mathcal{WD}_{K_v} \longrightarrow GL_n(\mathbb{C})$ (car $M$ est un prémotif).

**Lemme 6.2.3.** Si $G$ est un groupe compact et $\rho : G \longrightarrow GL_n(E_{\mathfrak{p}})$ est une représentation $\mathfrak{p}$-adique alors $\rho$ est équivalente à une représentation $\mathfrak{p}$-adique à valeurs dans $GL_n(\mathcal{O}_{E_{\mathfrak{p}}})$.

**Démonstration.** Le sous-groupe $GL_n(\mathcal{O}_{E_{\mathfrak{p}}})$ est un sous-groupe ouvert de $GL_n(E_{\mathfrak{p}})$ donc $H = \rho^{-1}(GL_n(\mathcal{O}_{E_{\mathfrak{p}}}))$ est un sous-groupe ouvert (car $\rho$ est continu) donc $H$ est d'indice fini dans $G$ (car $G$ est compact). Alors si on voit $GL_n(E_{\mathfrak{p}})$ comme le groupe des automorphismes linéaires de $E_{\mathfrak{p}}^n$ alors $\sum_{g \in H\backslash G} \rho(g)(\mathcal{O}_{E_{\mathfrak{p}}}^n)$ est un $\mathcal{O}_{E_{\mathfrak{p}}}$- réseau dans $E_{\mathfrak{p}}^n$ stable par $G$, ce qui nous fournit la représentation équivalente souhaitée. ■

**Proposition 6.2.4.** Soient $M$ un prémotif, $v$ une place de $K$ et $\sigma_{\iota M,v}$ une représentation essentiellement symplectique. S'il existe $\mathfrak{p} \nmid 2, l_v$ tel que $J = \sigma_{v,\mathfrak{p}}(I_{K_v})$ est fini alors $J$ est indépendant de $\mathfrak{p}$ ($\mathfrak{p} \nmid 2, l_v$) et

$$|J| \mid S_n(E)_v \text{ où } S_n(E)_v := \operatorname*{pgcd}_{\mathfrak{p} \nmid 2, l_v} S_{n,\mathfrak{p}}(E).$$

**Démonstration.** L'action de $\sigma_{\iota M,v}$ sur $I_{K_v}$ se factorise à travers $J = \sigma_{v,\mathfrak{p}}(I_{K_v})$ et par conséquent pour tout $\mathfrak{p} \nmid 2, l_v$ on a $J = \sigma_{v,\mathfrak{p}}(I_{K_v})$ et $J$ est indépendant de $\mathfrak{p}$. Si on pose $\sigma_{v,\mathfrak{p}|I_{K_v}}$ pour la restriction de $\sigma_{v,\mathfrak{p}}$ à $I_{K_v}$ alors la représentation $\sigma_{v,\mathfrak{p}|I_{K_v}}$ peut être considérée comme à coefficients dans $\mathcal{O}_{E_{\mathfrak{p}}}$ (d'après le lemme ci-dessus, car $I_{K_v}$ est un groupe compact) et même à valeurs dans $GSp_n(\mathcal{O}_{E_{\mathfrak{p}}})$ car $\sigma_{v,\mathfrak{p}}$ est essentiellement symplectique. On en déduit que pour tout $\mathfrak{p} \nmid 2, l_v$, $J$ s'injecte dans chacun des $GSp_n(\mathcal{O}_{E_{\mathfrak{p}}})$ (car $M$ est un prémotif) et donc $|J| \mid S_{n,\mathfrak{p}}(E)$ pour tout $\mathfrak{p} \nmid 2, l_v$. ■

**Corollaire 6.2.5.** Les nombres premiers qui divisent $|J|$ divisent $S_n(E) := \operatorname*{pgcd}_{\mathfrak{p} \nmid 2} S_{n,\mathfrak{p}}(E)$ (qui est indépendant de $l_v$).

**Démonstration.** Soit $\mathfrak{p}_v \mid l_v$ et $l$ un diviseur de $S_{n,\mathfrak{p}_v}(E)$ alors d'après le théorème de Dirichlet il existe $p$ premier (différent de $l_v$) tel que $l \mid p-1$ et donc $\forall r \in \mathbb{N}^*$, $l \mid p^r - 1$. En particulier, si $\mathfrak{p}$ est idéal premier au-dessus de $p$, $l$ divise $S_{n,\mathfrak{p}}(E)$. Ainsi les diviseurs premiers de $S_n(E)_v := \operatorname*{pgcd}_{\mathfrak{p} \nmid 2, l_v} S_{n,\mathfrak{p}}(E)$ sont les mêmes que ceux de $S_n(E) := \operatorname*{pgcd}_{\mathfrak{p} \nmid 2} S_{n,\mathfrak{p}}(E)$. ■

**Exemple 6.2.6.** Pour $E = \mathbb{Q}$ et $n = 2$ (le cas des courbes elliptiques), on obtient que pour tout nombre premier $p$ (avec $p \neq 2$), $|J| \mid p(p^2-1)$. Ce nombre est toujours divisible par $2^3 \times 3 = 24$ et on montre que $S(\mathbb{Q}) := S_2(\mathbb{Q}) = 24$ (car $S_{2,3}(\mathbb{Q}) = 24$). Donc dans ce cas les "mauvais" nombres premiers sont 2 et 3.

**Exemple 6.2.7.** Pour $E = \mathbb{Q}(\sqrt{5})$ et $n = 2$.
Tout d'abord $S_{2,\mathfrak{p}}(E) = q_{\mathfrak{p}}(q_{\mathfrak{p}}^2 - 1) = q_{\mathfrak{p}}(q_{\mathfrak{p}} - 1)(q_{\mathfrak{p}} + 1)$
On a que 5 est un résidu quadratique modulo $p \Leftrightarrow p \equiv \pm 1 \bmod 10$ (par la loi de réciprocité quadratique). On en déduit que les nombres premiers (différents de 2) qui :
- sont décomposés dans $E$ sont les nombres premiers congrus à 1 ou $-1$ modulo 10.
- sont inertes dans $E$ sont les nombres premiers congrus à 3 ou 7 modulo 10.

- sont ramifiés : il y a juste 5.
Ainsi si $\mathfrak{p}$ est une place au-dessus de $p$ et $q = N(\mathfrak{p})$ on a :

$$q = \begin{cases} p & \text{si } p \equiv \pm 1 \bmod 10 \\ p^2 & \text{si } p \equiv 3 \text{ ou } 7 \bmod 10 \\ 5 & \text{si } p = 5 \end{cases}$$

On en déduit que $\forall \mathfrak{p} \nmid 2$, 5 divise $S_{2,\mathfrak{p}}(E)$ et donc 5 divise $S_2(E)$.
Ainsi dans ce cas 2, 3 et 5 sont les "mauvais" nombres premiers (car 3 est inerte et $S_{2,3}(E) = 2^4 \times 3^2 \times 5$ ou encore $S_{2,(\sqrt{5})}(E) = 2^3 \times 3 \times 5$)

**Remarque 6.2.8.**
1. Pour $E$ quelconque et $p \leq n+1$ on a que $p$ divise $S_n(E)$ (petit théorème de Fermat). Ainsi tout les nombres premiers inférieurs ou égaux à $n+1$ sont des "mauvais" nombres premiers. Ce ne sont bien sûr pas les seuls (voir l'exemple ci-dessus $E = \mathbb{Q}(\sqrt{5})$ et $n = 2$ où 5 est un "mauvais" nombre premier).
2. Pour $E = \mathbb{Q}$, les "mauvais" nombres premiers sont précisément les nombres premiers inférieurs ou égaux à $n+1$. En effet, si $p > n+1 = 2m+1$ alors $\forall i \in \{1, .., m\}$, $p - 1 \nmid 2i$. On choisit alors un nombre premier $p'$ tel que $p'$ est une racine primitive modulo $p$ (c'est possible grâce au théorème de Dirichlet), on obtient $p \nmid p'^{2i} - 1$ $\forall i \in \{1, .., m\}$ et par conséquent $p \nmid S_n(\mathbb{Q})$. C'est ce cas là qui nous servira pour les prémotifs sur $\mathbb{Q}$ (notamment les courbes elliptiques et les variétés abéliennes).
3. Pour $E$ quelconque peut-on donner précisément les "mauvais" nombres premiers ? une borne (intéressante) ? Il est à noter, par exemple, que si les diviseurs premiers de $S_2(\mathbb{Q}(\sqrt{5}))$ sont 2, 3 et 5, ceux de $S_2(\mathbb{Q}(\sqrt{7}))$ sont simplement 2 et 3.

### 6.2.2 Détermination des nombres de Tamagawa.

On a toujours $M = \{(\sigma_\mathfrak{p}, V_\mathfrak{p})\}_\mathfrak{p}$ un prémotif essentiellement symplectique sur $K$. On suppose dorénavant que $p$ ne fait pas partie des "mauvais" nombres premiers (i.e $p \nmid S_n(E)$ et en particulier $p \nmid |J|$).

On rappelle la proposition générale suivante :

**Proposition 6.2.9.** Si $G$ est un groupe, $M$ un $G$-module et $H$ un sous-groupe distingué d'indice fini de $G$. Si $[G : H]$ est inversible dans $M$ alors :

$$H^1(G, M) \simeq H^1(H, M)^{G/H}.$$

**Démonstration.** Voir la proposition 10.4 p.85 de [7]. ■

**Proposition 6.2.10.** Si $\sigma_{\mathfrak{p},v}(I_{K_v})$ est fini et $p \nmid S_n(E)$ alors $p \nmid |J|$ et :

$$Tam(\sigma_{\mathfrak{p},v}) = 1.$$

**Démonstration.** D'après la proposition 6.1.3, le nombre de Tamagawa associé à une telle représentation $\sigma_{\mathfrak{p},v}$ est donné par

$$Tam(\sigma_{\mathfrak{p},v}) = \varpi_{E_\mathfrak{p}}^{\alpha}$$

où $\alpha = l_\mathfrak{p}\left((H^1(I_{K_v}, T)^{G_{K_v}})_{tors}\right)$.
On a la suite exacte suivante :

$$0 \longrightarrow I^0 \longrightarrow I_{K_v} \longrightarrow J \longrightarrow 0$$

donc d'après la proposition précédente avec $G = I_{K_v}$, $H = I^0$, $G/H = J$ et $M = T$ ($p \nmid |J|$ donc $|J|$ est inversible dans $T$) on déduit que $H^1(I_{K_v}, T) \simeq H^1(I^0, T)^J$. Or comme $I^0$ agit trivialement sur $T$, on a $H^1(I^0, T) \simeq Hom_{cont}((I^0)^{ab}, T)$ qui est sans $p$-torsion. Par conséquent, $\alpha = 0$ et $Tam(\sigma_{\mathfrak{p},v}) = \varpi^0_{E_\mathfrak{p}} = 1$. ■

**Corollaire 6.2.11.** Si $\sigma_{\mathfrak{p},v}(I_{K_v})$ est fini, $p \nmid S_n(E)$, $L_w$ est une extension galoisienne finie de $K_v$ et si on pose $\sigma_{\mathfrak{p},w} : G_{L_w} \longrightarrow GL(V_\mathfrak{p})$ alors :

$$Tam(\sigma_{\mathfrak{p},w}) = Tam(\sigma_{\mathfrak{p},v}) = 1,$$

autrement dit le nombre de Tamagawa reste inchangé lorsqu'on passe à une extension galoisienne finie de $K_v$.

### 6.2.3 Compatibilité entre nombres de Tamagawa et constantes de régulation

Soit $M = \{(\sigma_\mathfrak{p}, V_\mathfrak{p})\}$ un prémotif sur $K$ à coefficients dans $E$ (avec $\sigma_\mathfrak{p} : G_K \longrightarrow GL(V_\mathfrak{p}) \simeq GL_n(E_\mathfrak{p})$. On fait les hypothèses suivantes :
• Soit $v$ une place de $K$ ($v \mid l_v$) telle que $\sigma_v := \sigma_{\iota M,v}$ est une représentation essentiellement symplectique de poids $w$, modérément ramifiée du groupe de Weil $\mathcal{W}_{K_v}$.
• Soit $\mathfrak{p} \mid p$ une place de $E$ telle que $p \neq l_v$ et $p \nmid S_n(E)$ (en particulier $p > n+1$).
• L'image $\sigma_{v,\mathfrak{p}}(I_{K_v})$ est finie. Ainsi les facteurs premiers de $\sigma_{\mathfrak{p},v}(I_{K_v})$ divisent $S_n(E)$ (d'après le corollaire 6.2.5) et $\sigma_{\mathfrak{p},v}(I_{K_v})$ est d'ordre premier à $l_v$ (car $\sigma_v$ est modérément ramifié). En particulier $p \nmid |\sigma_{\mathfrak{p},v}(I_{K_v})|$.

On utilise les notations suivantes :
• La représentation $\tilde{\sigma}_v = \sigma_v \otimes \omega^{w/2}$ est une représentation symplectique modérément ramifiée du groupe de Weil $\mathcal{W}_{K_v}$.
• On écrit la décomposition de $\tilde{\sigma}_v^{ss}$ sous la forme suivante :

$$\tilde{\sigma}_v^{ss} = (\theta \oplus \theta^*) \oplus \bigoplus_{i=1}^{r} \tilde{\sigma}_i$$

où $\tilde{\sigma}_i = V_{\xi_i,-1}$.
• On a $\tilde{\sigma}_i = \rho_i \otimes ur_{\beta_i}$ où $ur_{\beta_i}$ un caractère non-ramifié de $G_i$ et $\rho_i = V_{\xi_i,1}$ une représentation orthogonale de $G_i$

**Définition 6.2.12.** On définit l'extension finie $L/K_v$ comme le compositum de :
• toutes les extensions quadratiques de $K_v$ qui sont non ramifiées ou modérément ramifiées.
• toutes les extensions modérément ramifiées $L_i$ telle que $\rho_i = V_{\xi_i,1}$ se factorise par $Gal(L_i/K_v)$.

**Remarque 6.2.13.** L'ordre de $\xi_i$ divise $|\sigma_{\mathfrak{p},v}(I_{K_v})|$ et donc on a $p \nmid |Gal(L_i/K_v)|$. Par conséquent, $p \nmid [L : K_v]$.

On pose enfin $G' = Gal(L/K_v) \simeq C \rtimes \langle \Phi \rangle$.

Soit $\tau$ une représentation auto-duale de $G = Gal(F/K_v)$ (où $F$ est une extension finie de $K_v$) et $r_G$ la représentation régulière de $G$.

On se ramènera au cas où $L \subset F$ (voir le corollaire 6.2.21 ci-dessous) et donc au cas où on peut voir $\sigma_v^{ss}$ comme une représentation de $G$.

On applique le corollaire 5.3.9 à $\sigma_v$ (et le fait que $\dim \tau = \langle r_G, \tau \rangle$) et on obtient :

$$W(\sigma_v \otimes \tau) = (\det \tau(-1))^{\frac{\dim \sigma}{2}} (-1)^{\langle \tau, \mathcal{V} \rangle}$$

où $\mathcal{V} = \bigoplus_i \mathcal{V}_i$ avec $\mathcal{V}_i = 1 \oplus \eta_{nr} \oplus \gamma_i \oplus \rho_i$, $\tilde{\sigma}_i = \rho_i \otimes ur_{\beta_i}$ (où $ur_{\beta_i}$ est un caractère non-ramifié de $G_i$ et $\rho_i = V_{\xi_i,1}$ une représentation orthogonale de $G_i$) et $\gamma_i = \begin{cases} r_G & \text{si } W(\sigma_i) = -1, \\ 0 & \text{si } W(\sigma_i) = 1. \end{cases}$

**Remarque 6.2.14.** La représentation $\mathcal{V}$ est une représentation sur $GL_n(E')$ avec $E'/E$ une extension finie telle que $\mathfrak{p}$ ne se ramifie pas dans $E'$. En effet, $\rho_i = V_{\xi_i,1}$ où l'ordre de $\xi_i$ divise $|\sigma_{\mathfrak{p},v}(I_{K_v})|$ et donc $\rho_i$ se factorise à travers le groupe de Galois d'une extension de degré $d_i$ de $K_v$ avec $p \nmid d_i$ et $p$ est non ramifié dans $\mathbb{Q}(\xi_i)/\mathbb{Q}$. L'extension $E'$ compositum de $E$ avec les $\mathbb{Q}(\xi_i)$ est une extension finie de $E$ où $\mathcal{V}$ est réalisable et $\mathfrak{p}$ ne se ramifie pas dans $E'$.

On rappelle que si $\Theta = \sum_i n_i H_i$ est une $G$-relation alors

$$\mathcal{D}_{\mathcal{V}}(\Theta) = C_\Theta(\mathcal{V}) = \prod_i \det \left( \frac{1}{|H_i|} \langle , \rangle \Big| \mathcal{V}^{H_i} \right)^{n_i} \in E'^{\times}/E'^{\times 2}$$

et si $\mathfrak{P}$ est une place de $E'$ au-dessus de $\mathfrak{p}$, on notera $ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}}(\Theta))$ pour $ord_{\mathfrak{P}}(\mathcal{D}_{\mathcal{V}}(\Theta))$. De plus, on notera $C_v(\Theta) = \prod_i Tam(\sigma_{\mathfrak{p},v_i})^{n_i}$ où $v_i$ est une place de $F^{H_i}$ au-dessus de $v$. On a $C_v(\Theta) = 1$ d'après le corollaire 6.2.11.

L'objectif de cette section est de démontrer le résultat principal de ce chapitre sous la forme du théorème suivant (ici on ne suppose pas que $L \subset F$) :

**Théorème 6.2.15.** Si $\Theta$ une $G$-relation, $\mathfrak{p} \mid p$ et $p \nmid l_v S_n(E)$ alors :

$$ord_{\mathfrak{p}}(C_v(\Theta)) \equiv ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}}(\Theta)) \equiv 0 \bmod 2$$

où $\mathcal{V}$ est défini ci-dessus. On notera parfois,

$$C_v \sim_{\mathfrak{p}} \mathcal{D}_{\mathcal{V}} \sim_{\mathfrak{p}} 1.$$

**Remarque 6.2.16.** On a d'après ce qui précède $C_v \sim_{\mathfrak{p}} 1$. L'objectif est donc de montrer que $\mathcal{D}_{\mathcal{V}} \sim_{\mathfrak{p}} 1$.

Dans le cas d'une courbe elliptique $A$ sur $K$ (un corps de nombres) avec $E = \mathbb{Q}$, $\mathfrak{p} = p$, $\sigma_{v,\mathfrak{p}} = V_p(A)^*$, $n = 2$, $p \geq 5$, $v \nmid p$ et $A$ admet bonne réduction sur une extension modérément ramifiée de $K_v$ (c'est automatique si $v \nmid 6$) on a la légère amélioration suivante (pour $p \geq 5$) du théorème 3.4.33 :

**Corollaire 6.2.17.** Si $L/K$ est une extension galoisienne de corps de nombres, $p \geq 5$ et $A/K$ est une courbe elliptique qui admet bonne réduction sur une extension modérément ramifiée de $K_v$ pour chaque place $v \mid 6$ de réduction additive où le groupe de décomposition en $v$ de $L/K$ n'est pas cyclique. Pour toute $G_{L/K}$-relation $\Theta$ on a :

$$(-1)^{\langle \tau, S_p(E/K) \rangle} = W(E/K, \tau) \text{ pour } \tau \in T_{\Theta,p}$$

**Remarque 6.2.18.** On pouvait en fait déjà déduire ce résultat en utilisant, une version légèrement plus forte de la formule de Rohrlich (qui pouvait se déduire de sa démonstration).

**Réduction au cas où $L \subset F$**

Comme promis, expliquons rapidement pourquoi on peut supposer que $L \subset F$. On rappelle que $G = Gal(F/K_v)$

**Lemme 6.2.19.** Supposons que $\mathcal{V}$ est $E[G]$-module et que $M/K_v$ est une extension galoisienne contenue dans $F$ (avec $H = Gal(F/M)$) alors on a :

$$ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}^H}(\Theta)) \equiv ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}}(\tilde{\Theta})) \mod 2 \text{ pour toutes } G/H\text{-relations } \Theta$$

où $\mathcal{V}' = \mathcal{V}^{Gal(F/M)}$, $\tilde{\Theta}$ est le relevé de $\Theta$ dans $G$ et $G/H = Gal(M/K_v)$.

**Démonstration.** Soit $\Theta = \sum_i n_i H_i$ une $G/H$-relation. On a la $G$-relation $\tilde{\Theta}$ : le relevé de $\Theta$ dans $G$. Comme les composantes $\bar{K}_v$-irréductibles de $\mathcal{V}^H$ sont précisément les $\bar{K}_v$-irréductibles de $\mathcal{V}$ qui se factorise par $G/H$, les composantes $\bar{K}_v$-irréductibles de $\mathcal{V} \ominus \mathcal{V}^H$ n'apparaissent dans aucun des $K_v[Gal(M/K_v)/H_i]$ et donc (d'après le lemme 3.4.12) $C_{\tilde{\Theta}}(\mathcal{V} \ominus \mathcal{V}^H) = 1$ puis $C_{\Theta}(\mathcal{V}^H) = C_{\tilde{\Theta}}(\mathcal{V})$ et $ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}}(\tilde{\Theta})) \equiv ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}^H}(\Theta))$. ■

**Remarque 6.2.20.** En combinaison avec la remarque 6.2.16, on a obtenu que :
Si $ord_{\mathfrak{p}}(C_v(\tilde{\Theta})) \equiv ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}}(\tilde{\Theta})) \mod 2$ pour toutes $G$-relations $\tilde{\Theta}$ alors :

$$ord_{\mathfrak{p}}(C_v(\Theta)) \equiv ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}^H}(\Theta)) \mod 2 \text{ pour toutes } Gal(M/K_v)\text{-relations } \Theta.$$

**Corollaire 6.2.21.** On peut supposer que $F$ contient $L$.

**Démonstration.** En effet, si $L$ n'est pas inclu dans $F$ alors $L \subset FL \subset (FL)^{Gal} = F'$ (clotûre galoisienne de $FL$). Et d'après le lemme précédent, si on montre le résultat pour $F'$ alors il vrai aussi pour $F$ (car $F/K_v$ est une extension galoisienne contenue dans $F'$). ■

Dorénavant, on suppose donc que $L \subset F$, on rappelle que $G = Gal(F/K_v)$ et on pose $G' = G/N = Gal(L/K_v)$.

**Démonstration du théorème 6.2.15**

Soit $\Theta$ une $G$-relation. On rappelle qu'on a supposé que $\mathfrak{p} \mid p$, $p \nmid S_n(E)$ (i.e $p$ ne fait pas partie des "mauvais" nombres premiers) et $p \neq l_v$.

On a que $\mathcal{V}$ est une représentation du groupe $G' = C \rtimes \langle \Phi \rangle$ (où $C$ est un groupe fini qui représente l'inertie, en particulier les diviseurs premiers de $|C|$ sont des diviseurs premiers de $S_n(E)$ donc distincts de $p$ par hypothèse).

**Lemme 6.2.22.** Pour démontrer le théorème 6.2.15, on peut se ramener au cas où le degré résiduel de $F/K_v$ est une puissance de 2.

**Démonstration.** Le nombre de Tamagawa reste trivial dans toute extension (voir la remarque 6.2.11). On a alors $C_v = (D, C_v)$ en itérant le 7. du théorème 3.4.20 (où $D \lhd G$ est le sous-groupe distingué tel que l'extension non-ramifiée maximale de degré impair de $K$ dans $F$ soit le corps fixe par $D$). Montrons que $\mathcal{D}_{\mathcal{V}} \sim (D, \mathcal{D}_{\mathrm{Res}_D \mathcal{V}})$.
Tout d'abord, d'après 3.4.23 $(D, \mathcal{D}_{\mathrm{Res}_D \mathcal{V}}) \sim \mathcal{D}_{Ind_D^G \mathrm{Res}_D \mathcal{V}}$. Or

$$Ind_D^G \mathrm{Res}_D \mathcal{V} \simeq \mathcal{V} \otimes Ind_D^G 1_D \simeq \mathcal{V} \oplus R$$

où $R = \mathcal{J} \oplus \mathcal{J}^*$ sur $\bar{\mathbb{Q}}$ et donc $\mathcal{D}_R \sim 1$ d'après le 2. du corollaire 3.4.11. Finalement,

$$(D, \mathcal{D}_{\mathrm{Res}_D \mathcal{V}}) \sim \mathcal{D}_{Ind_D^G \mathrm{Res}_D \mathcal{V}} \sim \mathcal{D}_{\mathcal{V}\oplus R} \sim \mathcal{D}_{\mathcal{V}}\mathcal{D}_R \sim \mathcal{D}_{\mathcal{V}}.$$

Maintenant, d'après le 1. du théorème 3.4.20, pour montrer que

$$C_v = (D, C_v) \sim_{\mathfrak{p}} (D, \mathcal{D}_{\mathrm{Res}_D \mathcal{V}}) \sim \mathcal{D}_{\mathcal{V}}$$

il suffit de montrer que $\mathcal{D}_{\mathrm{Res}_D \mathcal{V}}$ et $C_v$ coïncident sur les $D$-relations (c'est à dire lorsque le degré résiduel de $F/K_v$ est une puissance de 2). Autrement dit, pour montrer que $ord_{\mathfrak{p}}(C_v(\Theta)) \equiv ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}}(\Theta)) \equiv 0 \bmod 2$, il suffit de se resteindre au cas où le degré résiduel de $F/K_v$ est une puissance de 2. ■

**Proposition 6.2.23.** Avec les hypothèses ci-dessus, si $\Theta$ est une $G$-relation alors :

$$ord_{\mathfrak{p}}(C_\Theta(\mathcal{V})) \equiv 0 \bmod 2.$$

On pose $a_{\mathcal{V}}(\Theta) = \prod_i \det(\langle , \rangle \mid \mathcal{V}^{H_i})^{n_i}$ et $d_{\mathcal{V}}(\Theta) = \prod_i |H_i|^{-n_i \dim \mathcal{V}^{H_i}}$. On a donc

$$\mathcal{D}_{\mathcal{V}}(\Theta) = C_\Theta(\mathcal{V}) = a_{\mathcal{V}}(\Theta) d_{\mathcal{V}}(\Theta).$$

**Lemme 6.2.24.** Avec les hypothèses ci-dessus, si $\Theta$ est une $G$-relation alors :

$$ord_{\mathfrak{p}}(a_{\mathcal{V}}(\Theta)) \equiv 0 \bmod 2.$$

**Démonstration.** On a $a_{\mathcal{V}}(\Theta) = C_{\mathrm{Proj}_{G'}\Theta}(\mathcal{V}) \prod_i |H_i N/N|^{n_i \dim \mathcal{V}^{H_i}}$. Or d'après la proposition 3.4.16 $ord_{\mathfrak{p}}(C_{\mathrm{Proj}_{G'}\Theta}(\mathcal{V})) \equiv 0 \bmod 2$ et par ailleurs $p \nmid |G'|$ (en effet, $p \nmid |C|$, $p \neq 2$ et le degré résiduel de $F/K_v$ est une puissance de 2) donc $ord_{\mathfrak{p}}(\prod_i |H_i N/N|^{-n_i \dim \mathcal{V}^{H_i}}) \equiv 0 \bmod 2$. Finalement, on obtient $ord_{\mathfrak{p}}(a_{\mathcal{V}}(\Theta)) \equiv 0 \bmod 2$. ■

On va maintenant s'atteler à démontrer que

$$ord_{\mathfrak{p}}(d_{\mathcal{V}}(\Theta)) \equiv 0 \bmod 2 \text{ ou encore } d_{\mathcal{V}} \sim_{\mathfrak{p}} 1.$$

**Lemme 6.2.25.** Avec les hypothèses ci-dessus, on a :

$$ord_{\mathfrak{p}}(d_{\mathcal{V}}(\Theta)) \equiv ord_{\mathfrak{p}}\left(\prod_i (e_{H_i} f_{H_i})^{\dim \mathcal{V}^{H_i}}\right) \mod 2$$

où $e_H$ et $f_H$ sont respectivement l'indice de ramification et le degré résiduel de $F^H/K_v$.

**Démonstration.** On pose $d_{\mathcal{V}}(H) = |H|^{-\dim \mathcal{V}^H} (= |H|^{\dim \mathcal{V}^H}$ modulo les carrés). Montrons que $ord_{\mathfrak{p}}(d_{\mathcal{V}}(H)) \equiv 0 \bmod 2$. On peut remplacer $|H|$ par $[G : H]$. En effet si $\Theta = \sum_i n_i H_i$ alors $d_{\mathcal{V}}(\Theta) = \prod_i |H_i|^{n_i \dim \mathcal{V}^{H_i}}$. Or comme $\sum_i n_i \dim \mathcal{V}^{H_i} = 0$, on a :

$$\prod_i |H_i|^{n_i \dim \mathcal{V}^{H_i}} \prod_i [G : H_i]^{n_i \dim \mathcal{V}^{H_i}} = \prod_i |G|^{n_i \dim \mathcal{V}^{H_i}} = |G|^{\sum_i n_i \dim \mathcal{V}^{H_i}} = 1.$$

On en déduit que $\prod_i |H_i|^{n_i \dim \mathcal{V}^{H_i}} = \prod_i [G : H_i]^{n_i \dim \mathcal{V}^{H_i}}$ modulo les carrés. De plus, comme $[G : H_i] = e_{H_i} f_{H_i}$, on obtient :

$$\begin{aligned} ord_{\mathfrak{p}}(d_{\mathcal{V}}(\Theta)) &\equiv ord_{\mathfrak{p}}\left(\prod_i [G : H_i]^{\dim \mathcal{V}^{H_i}}\right) \mod 2 \\ &\equiv ord_{\mathfrak{p}}\left(\prod_i (e_{H_i} f_{H_i})^{\dim \mathcal{V}^{H_i}}\right) \mod 2. \end{aligned}$$

■

D'après le lemme 3.4.25, on sait que $\mathcal{D}_{r_G}(\Theta) \sim 1$ et donc que $\mathcal{D}_{1\oplus\eta_{nr}\oplus\rho\oplus r_G}(\Theta) \sim \mathcal{D}_{1\oplus\eta_{nr}\oplus\rho}(\Theta)$. Ainsi pour démontrer que $d_{\mathcal{V}} \sim_{\mathfrak{p}} 1$ dans le cas général, il suffit de le montrer dans le cas où $\tilde{\sigma} = \rho \otimes ur_\beta$ (avec $\rho = V_{\xi,1}$ pour un certain $\xi$) et $\mathcal{V} = 1 \oplus \eta_{nr} \oplus \rho$. On suppose donc désormais que :

$$\tilde{\sigma} = \rho \otimes ur_\beta \text{ et } \mathcal{V} = 1 \oplus \eta_{nr} \oplus \rho$$

On a (voir la proposition 5.1.3) que si $H \supset Gal(F/L)$ (i.e $F^H$ est un sous-corps de $L$) alors :

$$\dim(\rho^H) = \dim(V_{\xi,1}^H) = \begin{cases} 0 & \text{si } O(\xi) \nmid e_H \\ \text{pgcd}(f_H, m) & \text{si } O(\xi) \mid e_H \end{cases}$$

où $O(\xi) = |C|$ et $e_H$ et $f_H$ sont respectivement l'indice de ramification et le degré résiduel de $F^H/K_v$. Par ailleurs, on a que $\dim \eta_{nr}^H = 1 \iff 2 \mid f_H$ et que $f_H$ est une puissance de 2. D'après la définition de $L$,

$$2 \mid f_{F^H/K_v} \iff 2 \mid f_{F^H \cap L/K_v} \text{ et } O(\xi) \mid e_{F^H/K_v} \iff O(\xi) \mid e_{F^H \cap L/K_v}.$$

On en déduit que :

$$d_{\mathcal{V}} \sim_{\mathfrak{p}} \left(H \longrightarrow (e_H f_H)^{\dim \mathcal{V}^H}\right) = \left(G, I, \begin{cases} 1 & \text{si } 2 \mid f \text{ ou } O(\xi) \mid e \\ ef & \text{sinon} \end{cases}\right)$$

où $I$ est le sous-groupe d'inertie de $G$. Par ailleurs on a :

$$\begin{aligned} \left(G, I, \begin{cases} 1 & \text{si } 2 \mid f \text{ ou } O(\xi) \mid e \\ ef & \text{sinon} \end{cases}\right) &\overset{(6)}{\sim} \left(I, I, \begin{cases} 1 & \text{si } O(\xi) \mid e \\ e & \text{sinon} \end{cases}\right) \\ &\overset{(5)}{\sim} \left(I, W, \begin{cases} 1 & \text{si } O(\xi) \mid ef \\ ef & \text{sinon} \end{cases}\right) \end{aligned}$$

où $(n)$ correspond au point $n$ du théorème 3.4.20. On a alors dans le dernier terme que $e$ est une puissance de $l_v$ donc est premier avec $O(\xi)$, on en déduit que

$$\begin{aligned} d_{\mathcal{V}} &\sim_{\mathfrak{p}} \left(I, W, \begin{cases} 1 & \text{si } O(\xi) \mid f \\ ef & \text{sinon} \end{cases}\right) \\ &= \left(I, W, \begin{cases} 1 & \text{si } O(\xi) \mid f \\ e & \text{sinon} \end{cases}\right)\left(I, W, \begin{cases} 1 & \text{si } O(\xi) \mid f \\ f & \text{sinon} \end{cases}\right) \\ &\overset{(4)}{\sim} \left(I, W, \begin{cases} 1 & \text{si } O(\xi) \mid f \\ e & \text{sinon} \end{cases}\right) \\ &\sim_{\mathfrak{p}} 1 \end{aligned}$$

Ceci conclut la démonstration de la proposition 6.2.23 (et donc du théorème 6.2.15), en effet

$$ord_{\mathfrak{p}}(C_\Theta(\mathcal{V})) = ord_{\mathfrak{p}}(a(\Theta)) + ord_{\mathfrak{p}}(d(\Theta)) \equiv 0 \mod 2.$$

puis

$$\mathcal{D}_{\mathcal{V}} \sim_{\mathfrak{p}} 1 \sim_{\mathfrak{p}} C_v.$$

On peut maintenant énoncer le résultat suivant :

**Théorème 6.2.26.** Soit $\{(\sigma_{\mathfrak{p}}, V_{\mathfrak{p}})\}$ un prémotif de $Gal(\overline{K}/K)$ et $v$ une place de $K$ tel que $\sigma_{\iota M,v}$ soit une représentation modérement ramifiée, essentiellement symplectique du groupe de Weil $\mathcal{W}_{K_v}$. Si $n = \dim \sigma_{\mathfrak{p}}$, on demande que $p \nmid S_n(E)$ et $p \neq l_v$. Si $F/K_v$ est une extension galoisienne de groupe $G$ alors il existe un $E'[G]$-module $\mathcal{V}$ (voir la remarque 6.2.14) tel que :

1. $\frac{W(\sigma_{\mathfrak{p},v} \otimes \tau)}{W(\tau)^n} = (-1)^{\langle \tau, \mathcal{V} \rangle}$ pour toute représentation auto-duale $\tau$ de $G$.
2. On a la congruence suivante :

$$ord_{\mathfrak{p}}(\mathcal{D}_{\mathcal{V}}(\Theta)) \equiv ord_{\mathfrak{p}}(C_v(\Theta)) \equiv 0 \mod 2 \text{ pour toute } G\text{-relation } \Theta,$$

où $\mathcal{D}_{\mathcal{V}}(\Theta) = C_\Theta(\mathcal{V}) = a(\Theta)d(\Theta)$, $C_v(\Theta) = Tam(\sigma_{\mathfrak{p},v})(\Theta)$ avec $Tam(\sigma_{\mathfrak{p},v})(H) = Tam(\sigma_{\mathfrak{p},w_H})$ pour $w_H$ une place de $F^H$ au-dessus de $v$ et $\sigma_{\mathfrak{p},w_H} : G_{(F^H)_{w_H}} \hookrightarrow G_{K_v} \longrightarrow GL(V_{\mathfrak{p}})$.

On a vu que si $p > n+1$ alors $p \nmid S_n(\mathbb{Q})$, ce qui nous permet, en combinaison avec le théorème 3.4.26, de donner le théorème suivant dans le cas d'une variété abélienne.

**Théorème 6.2.27.** Soit $K/\mathbb{Q}_l$ un corps local, $F/K$ une extension galoisienne de groupe $G$, $A/K$ une variété abélienne de dimension $d$ qui acquière bonne réduction sur une extension modérément ramifiée de $K$ (ce qui est automatique si $l > 2d+1$) et $p$ un nombre premier tel que $p > 2d+1$ et $p \neq l$. Alors il existe un $\mathbb{Q}[G]$-module $\mathcal{V}$ tel que :

1. $\frac{W(A/K,\tau)}{W(\tau)^{2d}} = (-1)^{\langle \tau, \mathcal{V} \rangle}$ pour toute représentation auto-duale $\tau$ de $G$.
2. $ord_p(\mathcal{D}_{\mathcal{V}}(\Theta)) \equiv ord_p(C_v(\Theta)) \equiv 0 \mod 2$ pour toute $G$-relation $\Theta$.

### 6.2.4 Un résultat global

Soient un corps local $K_v$, $F_w/K_v$ une extension galoisienne, $A/K_v$ une variété abélienne et $p$ un nombre premier vérifiant les hypothèses du théorème 6.2.27. Alors si $\tau \in T_{\Theta,p}$ (voir corollaire 3.4.30 pour la définition) on a :

$$W(A/K,\tau) = \frac{W(A/K,\tau)}{W(\tau)^{2d}} = (-1)^{\langle \tau, \mathcal{V} \rangle} = (-1)^{ord_p C_\Theta(\mathcal{V})} = (-1)^{ord_p(C_v(\Theta))}$$

car si $\tau \in T_{\Theta,p}$ alors $W(\tau)^2 = 1$.

**Corollaire 6.2.28.** Soit $F/K$ une extension galoisienne de corps de nombres de groupe de Galois $G$, $A/K$ une variété abélienne, $v$ une place de $K$, $z$ une place de $F$ au-dessus de $v$ et $p$ un nombre premier. Supposons que $A/K_v$, $F_z/K_v$ et $p$ satisfont les hypothèses du théorème 6.2.27 alors pour tout $G$-relation $\Theta$ et $\tau \in T_{\Theta,p}$ on a :

$$W(A/K_v, \mathrm{Res}_{Gal(F_z/K_v)}\, \tau) = (-1)^{ord_p C_{w|v}(\Theta)}$$

où $C_{w|v}(H) = \prod_{w|v} C_w(A/F^H)$ et $\prod_{w|v} c_w(E/F^H)\omega(H)$,($c_w(E/F^H)$ est le nombre de Tamagawa local et $\omega(H) = \left| \frac{\omega^0_{A/K_v}}{\omega^0_{A/\left(F^{H_i}\right)_w}} \right|_{\left(F^{H_i}\right)_w}$ où $\omega^0_{A/K_v}$ est une différentielle de Néron).
De plus, si ces hypothèses sont vérifiées pour toutes places $v$ de $K$ alors

$$W(A/K_v, \tau) = (-1)^{ord_p C(\Theta)}$$

où $C(\Theta) = \prod_i (C_{E/F^{H_i}})^{n_i}$, $C_{E/F^{H_i}} = \prod_v C_{w|v}(H^i)$.

**Démonstration.** Voir le corollaire 3.4 p.48 de [18]. ■

Ce passage du local au global combiné avec le théorème 3.4.31 (qui lie $(-1)^{\langle \tau, S_p(A/K)\rangle}$ et $(-1)^{ord_p C(\Theta)}$) permet de déduire le théorème (global) annoncé à la fin de chapitre 3 :

**Théorème 6.2.29.** Soient $p$ premier, $p > 2d+1$, $L/K$ une extension galoisienne de corps de nombres et $A/K$ une variété abélienne de dimension $d$. Si on suppose que les places finies suivantes ont un groupe de décomposition cyclique :
· les places $v$ de réduction additive, au-dessus des nombres premiers inférieur ou égaux à $2d+1$.
· les places $v$ où $A$ n'a pas réduction semi-stable et $A$ a mauvaise réduction sur l'extension modérément ramifiée maximale de $K_v$.
· les places $v \mid p$.
alors pour toute $G_{L/K}$-relation $\Theta$ on a :

$$(-1)^{\langle \tau, X_p(A/K)\rangle} = W(A/K, \tau) \text{ pour } \tau \in T_{\Theta,p}.$$

# Index des notations

# Bibliographie


[1] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

[2] T. Barnet-Lamb, T. Gee, D. Geraghty, and R Taylor. Potential automorphy and change of weight. *Preprint*, 2010.

[3] A. Bartel and T. Dokchitser. Brauer relations in finite groups. *Preprint*, 2011.

[4] A. Bartel and T. Dokchitser. Brauer relations in finite groups ii - quasi-elementary groups of order $p^a q$. *Preprint*, 2011.

[5] Nicolas Billerey. Semi-stabilité des courbes elliptiques. *Dissertationes Math. (Rozprawy Mat.)*, 468 :57, 2009.

[6] Spencer Bloch and Kazuya Kato. $L$-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[7] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[8] D. Bump, J. W. Cogdell, E. de Shalit, D. Gaitsgory, E. Kowalski, and S. S. Kudla. *An introduction to the Langlands program*. Birkhäuser Boston Inc., Boston, MA, 2003. Lectures presented at the Hebrew University of Jerusalem, Jerusalem, March 12–16, 2001, Edited by Joseph Bernstein and Stephen Gelbart.

[9] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[10] Thomas de La Rochefoucauld. Invariance of the parity conjecture for $p$-selmer groups of elliptic curves in a $D_{2p}$-extension. *Bull. Soc. Math. France*, 139(4) :571–592, 2011.

[11] P. Deligne. Les constantes des équations fonctionnelles des fonctions $L$. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[12] P. Deligne. Les constantes locales de l'équation fonctionnelle de la fonction $L$ d'Artin d'une représentation orthogonale. *Invent. Math.*, 35 :299–316, 1976.

[13] P. Deligne. Valeurs de fonctions $L$ et périodes d'intégrales. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 313–346. Amer. Math. Soc., Providence, R.I., 1979. With an appendix by N. Koblitz and A. Ogus.

[14] P. Deligne and G. Henniart. Sur la variation, par torsion, des constantes locales d'équations fonctionnelles de fonctions $L$. *Invent. Math.*, 64(1) :89–118, 1981.

[15] Tim Dokchitser. Notes on the parity conjectures. *Notes based on the lectures given at CRM Barcelona in December 2009*, 2010.

[16] Tim Dokchitser and Vladimir Dokchitser. Parity of ranks for elliptic curves with a cyclic isogeny. *J. Number Theory*, 128(3) :662–679, 2008.

[17] Tim Dokchitser and Vladimir Dokchitser. Root numbers of elliptic curves in residue characteristic 2. *Bull. Lond. Math. Soc.*, 40(3) :516–524, 2008.

[18] Tim Dokchitser and Vladimir Dokchitser. Regulator constants and the parity conjecture. *Invent. Math.*, 178(1) :23–71, 2009.

[19] Tim Dokchitser and Vladimir Dokchitser. Self-duality of Selmer groups. *Math. Proc. Cambridge Philos. Soc.*, 146(2) :257–267, 2009.

[20] Tim Dokchitser and Vladimir Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math. (2)*, 172(1) :567–596, 2010.

[21] Tim Dokchitser and Vladimir Dokchitser. Root numbers and parity of ranks of elliptic curves. *Journal fur die reine und angewandte Mathematik (Crelle's Journal)*, (658), 2011.

[22] Jean-Marc Fontaine. Valeurs spéciales des fonctions $L$ des motifs. *Astérisque*, (206) :Exp. No. 751, 4, 205–249, 1992. Séminaire Bourbaki, Vol. 1991/92.

[23] Jean-Marc Fontaine and Bernadette Perrin-Riou. Autour des conjectures de Bloch et Kato : cohomologie galoisienne et valeurs de fonctions $L$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 599–706. Amer. Math. Soc., Providence, RI, 1994.

[24] A. Fröhlich and J. Queyrut. On the functional equation of the Artin $L$-function for characters of real representations. *Invent. Math.*, 20 :125–138, 1973.

[25] Alexander Grothendieck. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.

[26] Guy Henniart. Représentations du groupe de Weil d'un corps local. *Enseign. Math. (2)*, 26(1-2) :155–172, 1980.

[27] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[28] A. W. Knapp. Introduction to the Langlands program. In *Representation theory and automorphic forms (Edinburgh, 1996)*, volume 61 of *Proc. Sympos. Pure Math.*, pages 245–302. Amer. Math. Soc., Providence, RI, 1997.

[29] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.*, 69(4) :353–385, 1990.

[30] J. Martinet. Character theory and Artin $L$-functions. In *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 1–87. Academic Press, London, 1977.

[31] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47) :33–186 (1978), 1977.

[32] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2) :129–162, 1978.

[33] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3) :437–449, 1996.

[34] J.S. Milne. Class field theory. *Notes en ligne*.

[35] John W. Milnor and James D. Stasheff. *Characteristic classes*. Princeton University Press, Princeton, N. J., 1974. Annals of Mathematics Studies, No. 76.

[36] Jan Nekovář. On the parity of ranks of Selmer groups. II. *C. R. Acad. Sci. Paris Sér. I Math.*, 332(2) :99–104, 2001.

[37] Jan Nekovář. Selmer complexes. *Astérisque*, (310) :viii+559, 2006.

[38] Jan Nekovář. On the parity of ranks of Selmer groups. III. *Doc. Math.*, 12 :243–274, 2007.

[39] Jan Nekovář. On the parity of ranks of Selmer groups. IV. *Compos. Math.*, 145(6) :1351–1359, 2009. With an appendix by Jean-Pierre Wintenberger.

[40] Jan Nekovář and Andrew Plater. On the parity of ranks of Selmer groups. *Asian J. Math.*, 4(2) :437–497, 2000.

[41] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[42] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[43] David E. Rohrlich. The vanishing of certain Rankin-Selberg convolutions. In *Automorphic forms and analytic number theory (Montreal, PQ, 1989)*, pages 123–133. Univ. Montréal, Montreal, QC, 1990.

[44] David E. Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Math.*, 87(2) :119–151, 1993.

[45] David E. Rohrlich. Elliptic curves and the Weil-Deligne group. In *Elliptic curves and related topics*, volume 4 of *CRM Proc. Lecture Notes*, pages 125–157. Amer. Math. Soc., Providence, RI, 1994.

[46] David E. Rohrlich. Galois theory, elliptic curves, and root numbers. *Compositio Math.*, 100(3) :311–349, 1996.

[47] David E. Rohrlich. Galois invariance of local root numbers. *Mathematische Annalen*, 351 :979–1003, 2011. 10.1007/s00208-010-0626-z.

[48] David E. Rohrlich. Root numbers. In *Arithmetic of L-functions*, pages 353–448. AMS and IAS/Park City Mathematics Institute, 2011.

[49] Kark Rubin. Euler systems and kolyvagin systems. In *Arithmetic of L-functions*, pages 449–499. AMS and IAS/Park City Mathematics Institute, 2011.

[50] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[51] Maria Sabitova. Root numbers of abelian varieties. *Trans. Amer. Math. Soc.*, 359(9) :4259–4284 (electronic), 2007.

[52] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[53] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[54] Jean-Pierre Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978.

[55] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, second edition, 1989. With the collaboration of Willem Kuyk and John Labute.

[56] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[57] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88 :492–517, 1968.

[58] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[59] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[60] J. Tate. Number theoretic background. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 3–26. Amer. Math. Soc., Providence, R.I., 1979.

[61] J. T. Tate. Fourier analysis in number fields, and Hecke's zeta-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 305–347. Thompson, Washington, D.C., 1967.

[62] J. T. Tate. Local constants. In *Algebraic number fields : L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 89–131. Academic Press, London, 1977. Prepared in collaboration with C. J. Bushnell and M. J. Taylor.

[63] Richard Taylor. On the meromorphic continuation of degree two $L$-functions. *Doc. Math.*, (Extra Vol.) :729–779 (electronic), 2006.

[64] J. P. Wintenberger. Potential modularity of elliptic curves over totally real fields. *appendix to [39]*, 2009.

# Abstract

In this thesis, questions related to the parity conjecture are studied. We show the $p$-parity conjecture for a specific twist of an elliptic curve over a local field. We deduce global results concerning invariance (by some appropriate extensions) of the $p$-parity conjecture for an elliptic curve. With the objective to expand these results, a formula for root numbers of essentially symplectic and tamely ramified representations of the Weil group is shown. This result generalizes the one already known for elliptic curves with potentially good reduction. Finally, a first step is made toward the generalization on $p$-parity results whith the comparison of Tamagawa numbers and regulator constants for a premotif (with a few restrictions).



**Keywords.** Elliptic curves, abelian varieties, Birch and Swinnerton-Dyer conjecture, parity conjecture, $p$-parity conjecture, root numbers, regulator constant, Tamagawa numbers, premotifs, Weil group, Weil-Deligne group, $L$-functions.



# Résumé

Cette thèse porte sur des questions liées à la conjecture de parité. On démontre la conjecture de $p$-parité pour un certain twist d'une courbe elliptique sur un corps local. On en déduit des résultats globaux d'invariance de la conjecture de $p$-parité (pour une courbe elliptique) par certaines extensions. Avec l'objectif de généraliser les résultats précédents, on démontre une formule pour les signes locaux des représentations essentiellement symplectiques et modérément ramifiées du groupe de Weil. Cette formule généralise celle, déjà connue, pour les courbes elliptiques ayant potentiellement bonne réduction. Finalement, on fait un premier pas vers la généralisation escomptée en comparant les nombres de Tamagawa et les constantes de régulation pour certains prémotifs.



**Mots clefs.** Courbes elliptiques, variétés abéliennes, conjecture de Birch et Swinnerton-Dyer, conjecture de parité, conjecture de $p$-parité, signes locaux, constante de régulation, nombres de Tamagawa, prémotifs, groupe de Weil, groupe de Weil-Deligne, fonctions $L$.